Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2005-03

A multi-agent system for tracking the intent of surface contacts in ports and waterways

Tan, Kok Soon Oliver

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/2266

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A MULTI-AGENT SYSTEM FOR TRACKING THE INTENT OF SURFACE CONTACTS IN PORTS AND WATERWAYS

by

Kok Soon Oliver TAN

March 2005

Thesis Advisor:	John Hiles
Second Reader:	Russell Gottfried

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) A Multi-Agent System for Tracking the Intent of Surface Contacts in Ports and Waterways			**5. FUNDING NUMBERS**
6. AUTHOR(S) Kok Soon Oliver TAN			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Maritime security is especially critical for countries like Singapore, an island nation situated on the world's busiest shipping routes, whose economic prosperity is highly dependent on international trade from her busy port, petrochemical complexes and other high value units located along her coastline.

This thesis borrows the ideas and techniques suggested for identifying air threats in the Air Defense Laboratory (ADL) and employ them to identify asymmetric maritime threats in port and waterways. Each surface track is monitored by a compound multi-agent system that comprise of the several intent models, each containing a nested multi-agent system. The attributes that define intent models of friendly, neutral, unknown and potentially hostile surface contacts are obtained from movement and communication protocols defined by the Vessel Traffic Information System (VTIS), maritime navigation rules and cues for surface warfare threat assessment. The underlying cognitive mechanism of the models is conceptual blending.

The study includes a simulation of a mock VTS for the port of Singapore and surrounding waterways to test the ability of the models to compress data and information regarding multiple simulated surface contacts into integration networks and then determine the surface contacts' intent through the expansion of the integration networks.

14. SUBJECT TERMS Threat Assessment, Maritime Protection, Multi-agent Systems, Intent Tracking, Conceptual Blending			**15. NUMBER OF PAGES** 90
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A MULTI-AGENT SYSTEM FOR TRACKING THE INTENT OF SURFACE CONTACTS IN PORTS AND WATERWAYS

Kok Soon Oliver TAN
Civilian, Defence Science & Technology Agency, Singapore
M. Tech., National University of Singapore, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN MODELING, VIRTUAL ENVIRONMENTS, AND SIMULATION (MOVES)

from the

NAVAL POSTGRADUATE SCHOOL
March 2005

Author: Kok Soon Oliver Tan

Approved by: John Hiles
Thesis Advisor

Russell Gottfried
Second Reader

Rudy Darken
Chair, MOVES Academic Committee

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Maritime security is especially critical for countries like Singapore, an island nation situated on the world's busiest shipping routes, whose economic prosperity is highly dependent on international trade from her busy port, petrochemical complexes and other high value units located along her coastline.

This thesis borrows the ideas and techniques suggested for identifying air threats in the Air Defense Laboratory (ADL) and employ them to identify asymmetric maritime threats in port and waterways. Each surface track is monitored by a compound multi-agent system that comprise of the several intent models, each containing a nested multi-agent system. The attributes that define intent models of friendly, neutral, unknown and potentially hostile surface contacts are obtained from movement and communication protocols defined by the Vessel Traffic Information System (VTIS), maritime navigation rules and cues for surface warfare threat assessment. The underlying cognitive mechanism of the models is conceptual blending.

The study includes a simulation of a mock VTS for the port of Singapore and surrounding waterways to test the ability of the models to compress data and information regarding multiple simulated surface contacts into integration networks and then determine the surface contacts' intent through the expansion of the integration networks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The field of maritime security and protection is relatively new but increasingly important and I am practically jumping off the deep end in attempting to develop a MAS design for surface contact intent tracking. I would like to thank Professor John Hiles for giving me the courage and inspiration to take on this bold endeavor.

I would also be quite lost at sea without the guiding beacon provided by LCDR Russell Gottfried to navigate with. I would like to thank him for his invaluable expertise and knowledge in the domain of maritime protection.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The attacks on the Khobar Towers in 1996, the terrorist bombing of the USS COLE in Yemen in 2000, and the bombing of the French-flagged supertanker *Limburg* in the Arabian Sea off Yemen's Hadramut coast in October 2002 have brought into focus the reality of asymmetric maritime terrorism and the vulnerabilities of ports, waterways and shipping routes. Maritime security is especially critical for countries like Singapore, an island nation situated on the world's busiest shipping routes, whose economic prosperity is highly dependent on international trade from her busy port, transshipping container terminals, petrochemical complexes and other high value units located along her coastline.

This thesis is inspired by similar work done in the area of air threat assessment. The thesis borrows the ideas and techniques suggested for identifying air threats in the Air Defense Laboratory (ADL) and employ them to identify asymmetric maritime threats in the relatively less investigated but very important area of port and waterways security.

Implementing four intent models of surface contacts, Friend, Neutral, Unknown, and Potentially Hostile, a compound multi-agent system (MAS) monitors every surface contact by representing each contact with a Track agent. Each Track agent contains another nested multi-agent system that comprise of the four intent models. The underlying cognitive mechanism for the intent models is conceptual blending, also known as conceptual integration. The theory of conceptual blending is one possible explanation of how humans are able to think: giving meanings to external information and events, compressing the information into integration networks and eventually learning and gaining experience.

Vessel Traffic Service manuals, international and inland maritime navigation rules, surface threat assessment requirements reports and known terrorist tactics serves as source material for the attributes that define the intent models of friendly, neutral, unknown and potentially hostile surface contacts in ports and. Currently these models use the following information to identify hostility and potential threats before they are able to strike:

1. the movement and communication rules used by vessels registered with the Vessel Traffic Systems (VTS) used in ports and waterways, and
2. the cues for surface warfare threat assessment that is used by experienced surface warfare officers.

This study features a mock VTS-C2 system to evaluate the MAS. Similar to the ADL, simulations of scenarios with hostilities in the port of Singapore and surrounding waterways test the ability of the models to identify the intent of multiple simulated surface contacts by blending data and information into integration networks. Expansion of the integration networks can yield the intent identification process of a surface contact used by the compound MAS. Face validation by domain experts generated very encouraging results.

The thesis does not cover the issue of track detection. The issue of tactical actions resulting from a potentially hostile track identified by the system is also beyond the scope of this thesis.

I. INTRODUCTION

A. BACKGROUND

The Port of Singapore is one of the busiest in the world, in terms of both gross shipping tonnage and twenty-foot equivalent unit (TEU) container throughput [1] [2]. It is the focal point of approximately 200 shipping routes which connect Singapore to more than 600 ports in 120 countries and there are about 1,000 ships in the port at any time [1]. Located a stone's throw away from the port is the Singapore Cruise Center, the cruise hub of the Asia Pacific for passenger liners as well as regional and domestic ferries [1]. Situated on nearby off-shore islands are also oil terminals and refineries managed by many multi-national petroleum companies [3]. Every day, hundreds of vessels of all sizes, ranging from small dinghies and bumboats to barges and fishing trawlers to large cruise liners and oil tankers, traverse the deep but narrow band of sea surrounding the island state as they go about performing their daily activities [4].

While the Maritime Port Authority (MPA) of Singapore is responsible for overseeing and monitoring the traffic in the sea lanes vessel movements, ensuring navigational safety and managing the marine environment in the port [5], the defense of the harbor against potential sea threats falls in the hands of the Singapore Police Coast Guard (PCG) and the Republic of Singapore Navy (RSN). The PCG enforces the law and maintains order in Singapore Territorial Waters (STW). They also conduct Search and Rescue and assist other maritime agencies such as the MPA [6]. The RSN is responsible for the overall defense of the Singapore territorial waters against sea-borne threats and to protect the sea lines of communications that covers the Singapore Straits and its access routes [7].

Together, the PCG and RSN protect the STW, covering an area of more than 200 square nautical miles, larger than of the Singapore mainland. They oversee a territory that stretches as far as the Horsburgh Lighthouse in the east to the Sultan Shoal in the west, Raffles Lighthouse in the south to the narrow Johor Strait in the north [6]. The PCG and RSN have integrated their operational responses since 1993. Both agencies work alongside each other to combat and deter sea robbery, piracy and hijack. This co-

ordinated approach has not experienced a single case of sea robbery in Singapore waters since July 1990. [8]

Although well guarded by the PCG and RSN, the security of the waters around the STW remains tenuous. The Strait of Malacca has received attention for attacks against vessels at sea [9]. This has stemmed from both the strategic location of the Strait as an artery for over 50 per cent of international trade and 80 per cent of Japan's oil supplies; and for its close proximity to Singapore [9]. However, in terms of relative risk, the Strait of Malacca is less dangerous the zone east of Bintan Island. Bintan and neighboring Batam Island, a free-trade zone that is just outside the STW, have long been recognized as venues where organized crime syndicates and pirate gangs meet, do business and plan major attacks [9]. In these waters, shipping tends to concentrate and slow as it approaches the Strait of Singapore, presenting what one intelligence official described as "sitting ducks" [9].

The kinds of maritime threats and the ways these threats can be executed are numerous and unpredictable. For example, terrorists on a perfectly legitimate cruise liner can scuttle it when it is approaching the cruise center, potentially shutting down the waterways to the port as well. It is also possible for terrorists to hijack a vessel and ram it against the cruise center, the container terminal or an oil refinery [10] Another possibility is for terrorists to fire rocket-propelled grenades (RPG) or piercing light anti-tank weapons at passing oil tankers or refineries from commercial fishing trawlers or ferries [11]. Deception and surprise are also tools used by maritime terrorists against naval ships. Even if a naval ship was fitted with long-range guns, a terrorist group can conduct a “wolf-pack” attack where a cluster of terrorist craft will simultaneously approach a target craft from multiple directions [11].

The increase in piracy attacks is particularly worrying due to the vulnerability to terrorism of Singapore’s strategically important waterway. Singapore’s defense minister, Teo Chee Hean, warned, “the damage could be horrific if terrorists turned supertankers … or chemical carriers into floating bombs” [12]. Because the coastal waters around Singapore play such a vital role as one of the country’s economic pillars, protection of these waterways is imperative.

B. EFFORTS TO ENHANCE INTERNATIONAL MARITIME SECURITY

In November 2001, the International Maritime Organization (IMO) Assembly adopted a resolution to develop appropriate measures to enhance maritime security in order to preclude a terrorist attack from the sea. In December 2002, the IMO adopted new maritime security measures that included amendments to the 1974 Convention of Safety of Life at Sea (SOLAS 74) as well as a new mandatory International Ships and Port Facilities Security (ISPS) Code [13]. Some of the amendments that have already been adopted or extended by the MPA include:

1. installation of shipboard Automatic Identification Systems (AIS) [14] [15],

2. equipment of silent ship-to-shore security alert systems [16],

3. request of information related to ship security that a ship may be required to provide prior to entering the port and initial inspection of the ship when in the port [17],

4. empowering port state control officers to take appropriate measures, including delay, restriction of operations, denial of entry or expulsion from port, in response to any non-compliance of the requirements of Chapter XI-2 of the SOLAS 74 or the ISPS Code [17],

5. requiring vessels to maintain continuous record of registration, ownership and other information that can be used by port control officers to assess any security risk posed by a vessel [18], and

6. extending the ISPS Code to include mandatory compliance by small vessels and harbor craft that solely operates within the port limits [19].

Singapore has moved to meet this threat to national security. Besides seeking to improve port security, the Singapore government has also instituted a range of new measures, including providing escorts for high-value vessels within its waters and conducting special forces training aimed at retaking a hijacked vessel. In order to increase awareness beyond its own waters, Singapore has also hosted a series of international conferences and meetings focused on maritime security [9].

C. THE OBJECTIVES OF THE SURFACE CONTACT INTENT TRACKING SYSTEM FOR HARBOR AND WATERWAYS SECURITY

How can surface contact intent be modeled in a multi-agent system (MAS) for the identification of potentially hostile behaviors and potential threats in ports and waterways? This is the first research question that this thesis hopes to answer. The three main agencies that provide surveillance of the waters around Singapore are the MPA, PCG and RSN are focused on different areas and regions so each agency may develop different surveillance blind spots. A composite surveillance picture may help to mitigate the effects of the surveillance blind spots for each agency. Many information and intelligence sources contribute to a composite surveillance picture. Examples of some important information sources include the Port Traffic Management System (PTMS) and the Vessel Traffic Information System (VTIS) that are used to manage vessel traffic in harbors and waterways [20]. Some other information sources may include civilian and military sensors, coastal patrols, unmanned aerial vehicles (UAVs), unmanned surface vehicles (USVs), spot reports, visual sightings, and general communication reports from coastal patrols. A MAS can produce a common composite surveillance picture of the territorial waters about Singapore by compiling and correlating all information sources.

The second research question for this thesis is: Are the models sufficiently realistic to be used as a decision aid in maritime security? With a monthly record of almost 11,000 arrivals of vessels, totaling an upwards of 75 gross tons, into the Port of Singapore [4], and many unrecorded smaller leisure and fishing vessels, the number of surface contacts presented on a common composite surveillance picture will be overwhelming. It would be very difficult for port control officers to be able to identify surface contacts with mischievous or potentially hostile intent before they are allowed to strike.

Knowing the identity of surface contacts is insufficient for discovering potential incoming threats to civilian or military assets, as in the case of a high-jacked vessel. The MAS performs threat assessment with track attributes and cues that are considered by human surface warfare experts, and monitors for suspicious behaviors over time among all surface contacts that are within the port and territorial waters of Singapore. Such behaviors may include loitering, violations of international navigation rules,

encroachment into restricted areas, aggressive maneuvers and even unusual coordinated activities among surface contacts.

By integrating intelligence and information from as many sources as possible, the designer hope the MAS achieves its primary objective: to help the human operator sieve through the hundreds of surface contacts by integrating rules, information sources and intelligence into surface contact intent models, and immediately highlight when any suspicious or potentially hostile surface contacts have been identified. The system is expected also to consider the information provided under the new amendments to the SOLAS convention [13]. These include the shipboard AIS and security alert system, declaration of security and security logs, registries of vessel registration, vessel ownership, cargo manifests, and vessel transit schedules.

D. SCOPE OF THE CURRENT STUDY

Detection of low observables such as small leisure and fishing vessel is a problem in the maritime domain even with the most advance maritime sensor technology. Although the MAS will not be concerned with solving this problem, the ability of the MAS to identify the intention of tracks by consolidating available and incomplete information will be helpful in highlighting suspect low observables. Emerging profiles of interest require further investigation by other resources such as UAVs, USVs or coastal patrols.

Upon identifying potential threats, the system immediately alerts users of the system such as vessel traffic controllers, possibly from the MPA, at the Vessel Traffic Center. Follow-on decisions, like alerting higher authorities or raising a warning to the public, lie with the user. The processes involved in deciding countermeasures to tackle a threat once it has been identified are beyond the scope of this system.

E. RELATED WORK IN OTHER THREAT INTENT IDENTIFICATION SYSTEMS

The MAS is partly inspired by the work done by Ozkan [21] in the autonomous agent-based simulation system for air-threat assessment. This work incorporated the idea of conceptual blending [22], together with the research of Amori [23] and Liebhaber [29] in airborne threat assessment, to build a model that is capable of predicting the intent of air tracks. Besides predicting track intent, the system is also able to identify coordinated activities between air tracks. The idea and mechanisms for conceptual blending will be covered in more detail in Chapter II. Similarly, the MAS also incorporate ideas from Liebhaber's preliminary research in surface warfare threat assessment [30] which is described in more details in Chapter II as well.

Chapter III describes in detail the architecture of the compound MAS developed for tracking the intent of surface contacts moving in harbors and waterways. The agents use basic track data and conceptual blending operations to infer more information about a track. Intent models use the track information to compute the current intent of a surface contact. Chapter IV describes the mock VTS-C2 (Vessel Traffic Service-C2) system that is developed to test the MAS against scenarios incorporating hostility that may exist in a harbor and surrounding waterways. Experts in the domain of surface warfare threat assessment and harbor security evaluate the system. The results are presented in Chapter IV. Chapter V concludes the thesis by discussing recommendations and suggestions for improving the MAS.

II. THEORY BACKGROUND

A. INTRODUCTION

This chapter will provide a background into the human decision making process in real-life situations under stress of time and resources. This will be followed by a discussion of threat assessment processes that has been used by experts in the military. Several multi-agent models for threat assessment will be presented, including a multi-agent system that uses conceptual blending which is a novel theory about how humans rationalize the events that are happening around them.

B NATURALISTIC DECISION MAKING

Traditional decision research has focused on only one part of decision making, referred to as the decision event, where an individual makes a choice after considering a known and fixed set of alternatives and weighing the likely consequences of each available choice [24]. However, research [25] into the naturalistic decision making (NDM) process of fireground commanders in real-life situations showed that the decision event model does not correspond with how the commanders actually make decisions. Instead of making choices, considering alternatives or assessing probabilities, the commanders acted and reacted based on prior experience, generating, monitoring and modifying plans to meet the needs of the situations.

Most NDM models are characterized by a process that involves matching the pattern of a situation to sets of actions, and then selecting and evaluating an action with respect to goals and plans. Table 1 shows eight important factors characterize the settings of these NDM models. Though it is not necessary that all eight factors be significantly present in the same setting, it is the combination of several of these factors that will complicate the decision task in a realistic setting [24].

1.	Ill-structured problems
2.	Uncertain dynamic environments
3.	Shifting, ill-defined, or competing goals
4.	Action/feedback loops may help the decision maker generate corrective actions or adjust their plans based on early mistakes
5.	Significant time pressure on the decision maker
6.	High stakes on the outcomes of the decisions made
7.	Multiple players involved in the decision making process
8.	Organizational goals and norms that guides the decision maker

Table 1. Important factors in NDM models

C. THE RECOGNITION-PRIMED DECISION MODEL

One study of command-and-control performance led to the Recognition-Primed Decision (RPD) model of rapid decision making that explains how decisions are made by experts without having to compare all options. The RPD appears to be used for up to 96% of expert decisions [27]. Figure 1. presents a complex RPD model that fuses two processes: situation assessment and mental simulation.

A recognition strategy for situational assessment is used by an expert decision maker in a changing situation. These include plausible goals that can be achieved, critical cues from the observed situation, expectations about tasks and outcomes that can be accomplished within a limited time, and finally the generation of an obvious course of action. Mental simulation, also known as imagery, is next used to evaluate the course of action. The evaluation may reveal flaws that need modification or inadequacies in an option that can be rejected and the next most typical course of action is used [25].

D. THREAT ASSESSMENT

Situation awareness, as defined by Endsley [28], is the state of knowledge achieved by "the perception of the elements in the environment, the comprehension of their meaning, and the projection of their status in the near future." Within the framework of NDM, it appears that the processes of threat assessment and situation awareness share many common elements and that threat assessment may be an instance of situation assessment [29].

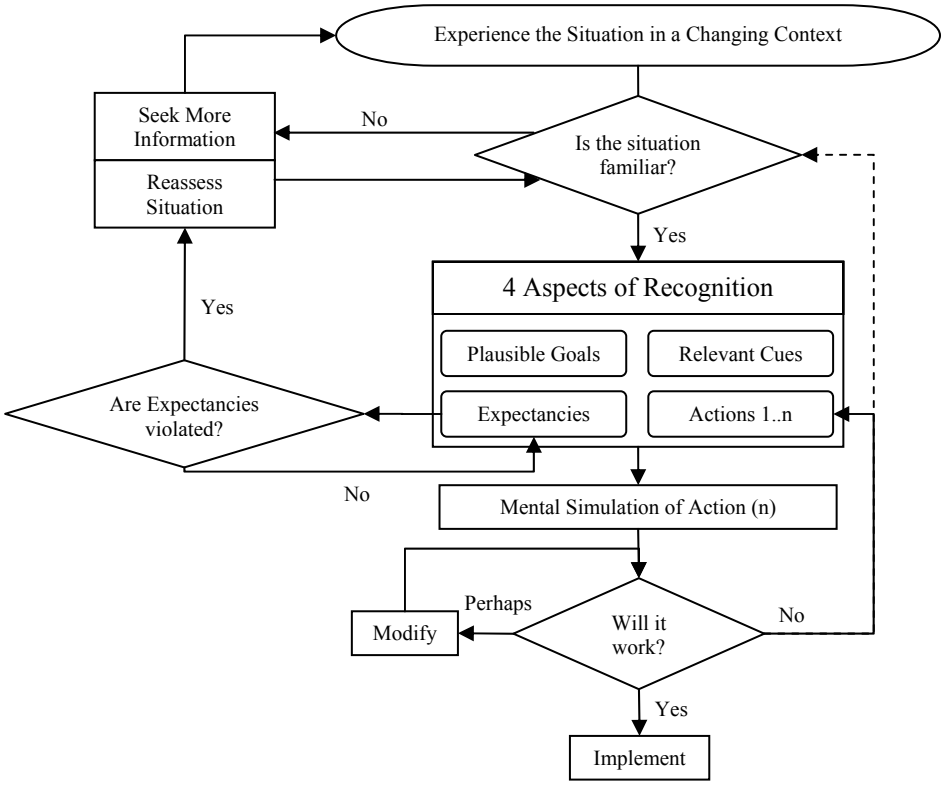

Figure 1. A complex RPD model (From Ref: 27)

The study in airborne threat assessment by Liebhaber and Smith [29] offered an insight into the process of building situation awareness by expert Air Defense officers. Results from their research suggested that threat assessment is an evaluation process that compares the degree of fit between input data and the expected data values based on profiles (schemas), as shown in Figure 2. This is similar to situation assessment in the NDM framework. Profiles are used to organize and evaluate information, to make

judgments. It is found that when data atypical of a profile is found, the experts will attempt to provide explanation for the inconsistencies with the profile rather than change profiles.

The profiles in airborne threat assessment are schemas that specify the expected behaviors of a class of aircraft. The air defense experts use these profiles to evaluate track data about an aircraft. Up to 22 major factors are used in these profiles, including electromagnetic signal emissions, Identification Friend or Foe (IFF) values, origin, speed, altitude, intelligence reports, and weapon envelope. Every profile consists of a subset of these factors and a corresponding set of expected data values. The expected data may be in the form of a range of values, or as threshold values.

An evaluation process compares the degree of fit between input data and the expected values based on the profiles. The resulting threat level of an aircraft depends on the evaluated degree of match between expected and actual input data values. The threat level increases as the degree of cognitive dissonance increases. There is evidence of geopolitical situation bias playing an indirect role of deciding the threat level in the threat assessment process [29]. The bias modifies the range of acceptable input values and reduces the tolerance for deviations from expected behaviors. The reduced tolerance for deviation led to more mismatches which in turn resulted in higher threat levels being reported.

Using similar data collection process and algorithm development, Liebhaber and Feher has conducted a preliminary investigation of cues that experienced surface warfare personnel use to evaluate the threat level of nearby surface ships in both littoral and open sea environments [30]. The objectives of the investigation were to:

1. find the level of threat associated with different types of ships,
2. identify the relationship between specific values of cues and the corresponding perception of threat,
3. rank the cues in order of importance or relevance to threat assessment, and
4. develop an algorithm for surface threat assessment.

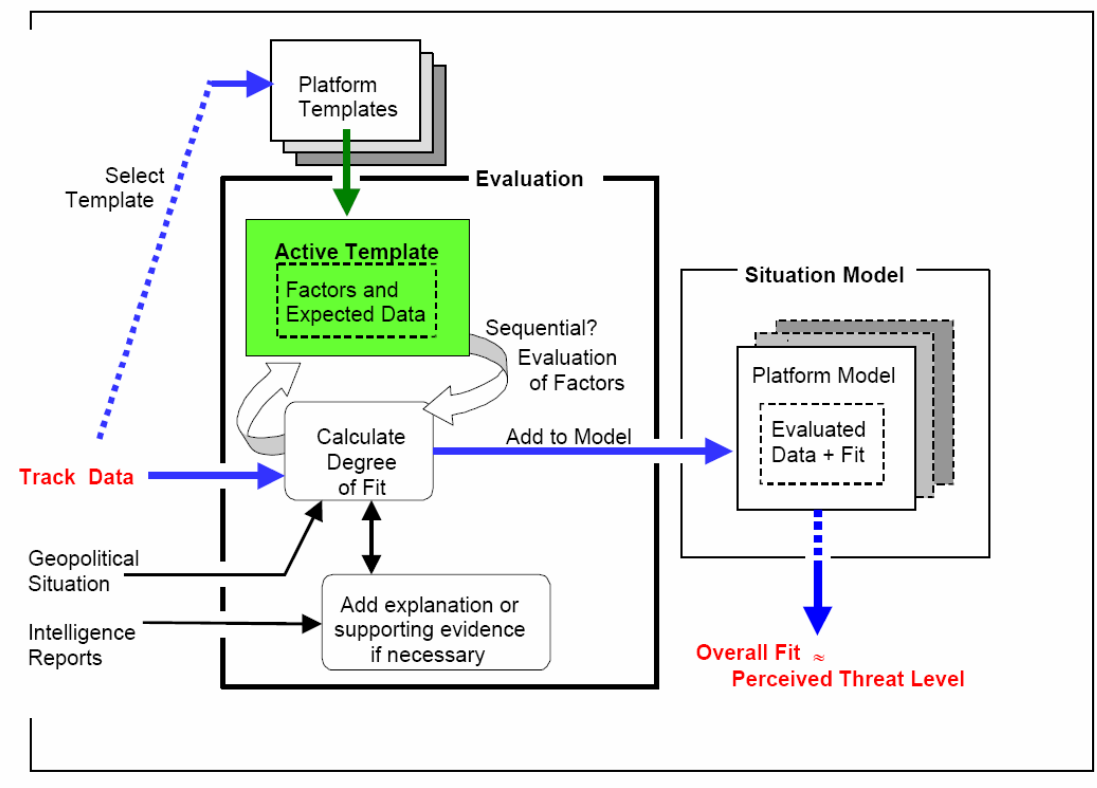

Figure 2. Cognitive-based Model of Threat Assessment (From Ref: 29)

Initial threat levels are established from a set of categories that includes (non-exhaustive) origin, ship structure, and type of military or commercial vessels, as shown in Table 2.

Flag/Origin	Hull Type	Military	Commercial/Private Vessels
1. Friend	1. Type 1	1. Carrier	1. Sealift
2. Hostile	2. Type 2	2. Patrol/Escort	2. Fishing
3. Unknown	3. Type 3	3. Service Craft	3. Repair/Rescue
		4. Other Auxiliary	4. Pleasure/Small

Table 2. Categories used to establish initial threat level

After categorizing the vessel, the cognitive model assigns threat level change ratings (TCRs) to these baseline threat levels from 15 environment and track data. The cues are ranked in relative importance to the assessment of threat. A TCR describes the relationship between the cued data and the perceived changes to the baseline threat levels with a magnitude of change. A positive TCR represents a rise in threat level while a negative TCR will result in a fall in threat level. Table 3 summarizes some of the TCRs used.

1.	Speed
2.	Course/Heading from Own-Ship
3.	Closest Point of Approach (CPA)
4.	Recent maneuvers/history
5.	Electronic Support Measures (ESM)/Radar Emitter
6.	Voice communication with track
7.	Range/Distance from Own-Ship
8.	On/Near Sea Lane/Traffic Lane
9.	Destination of track
10	Potential or Known Weapon Envelope of track
11.	Regional Intelligence
12.	Coordinated Activity

Table 3. Threat Level Change Ratings

Finally, the model derives a rule-based surface threat algorithm based on a set of empirical and observational studies on naval air threat assessment by Air Defense officers in the earlier study [30].

E. CONCEPTUAL BLENDING

Conceptual Blending, proposed by Fauconnier and Turner, is a theory about how humans process the information coming from the environment and how humans rationalize the events happening around them. The theory of conceptual blending, also known as conceptual integration, is one possible explanation of how humans think: give meaning to external information and events, integrate the information, and eventually learn and gain experience. The key process in the theory is blending; humans are unconsciously but constantly blending when talking, listening, imagining and in every other aspect of human life [22].

Blending is a set of mental operations for combining cognitive models in a network of discrete mental spaces. Mental spaces are small conceptual packets constructed as we think and talk for the purpose of understanding and action. Mental spaces are connected to long-term schematic knowledge called "frames" such as the frame of sailing along a ferry route or inside a maritime traffic separation scheme (TSS), and to long-term specific knowledge such as a memory of an event such as past track incursions into Area-To-Be-Avoided (ATBA) zones. Within the mental spaces are elements of these types of knowledge that are structured by frames. Mental spaces are interconnected in working memory which can be modified dynamically and they can be used to model dynamic mappings in thought and language [22].

Building a conceptual integration network involves setting up several mental spaces [22]. A minimal integration network is shown in Figure 3. The network is comprised of several components:

1. Two input mental spaces, represented by circles, with cross-space mapping, represented by the solid lines, to connect counterparts in these input mental spaces.

2. A generic mental space that captures the structure that input spaces share which is in turn map onto, represented by the dotted lines, each of the input i.e. a given element in the generic space maps onto paired counterparts in the input spaces.

3. The blended space, or just simply called "the blend", is the mental space onto which, during blending, the structure from the input mental spaces, indicated by the dotted lines, is projected. However not all elements and relations from the input spaces

are projected into the blend. Generic spaces are used together with the generic structures they contain to guide the selective projection of elements from the input spaces into blended spaces. The blended spaces will contain more specific structures, based on information from the input mental spaces.

4. In the blend, emergent structure, represented by the solid square in the blended space, may arise in the blend but not exist in any of the mental spaces. It can be generated in three ways:

i. through *composition* of projections from the inputs [22],

ii. through *completion* based on independently recruited frames and scenarios [22], and

iii. through *elaboration* ("running the blend") i.e. treating the blends like mental simulations that run according to the principles that have been established for the blend [22].

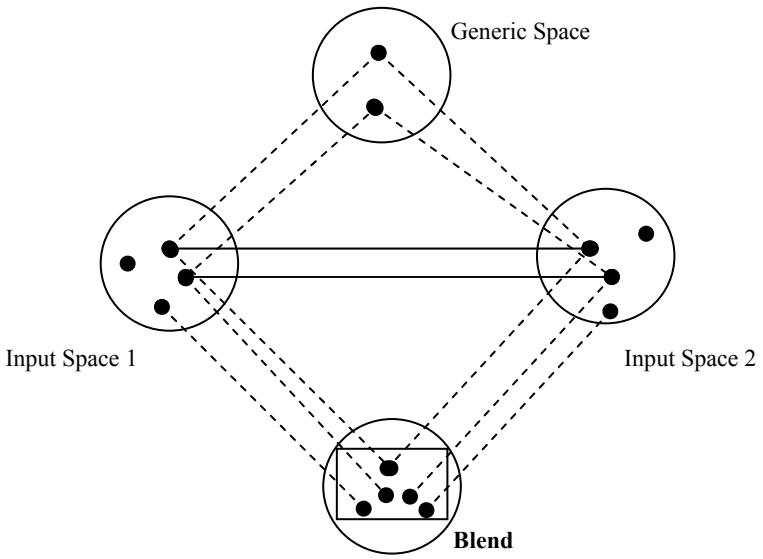

Figure 3. A Basic Conceptual Integration Network

The new blended space, together with its emergent structure can next participate as an input space of another similar minimal network. Any mental space can participate

in multiple networks. Complex integration networks, as shown in Figure 4. , can be built with arrays of mental spaces connected through blending operations. These integration networks have coherent structures that represent the way human think and make meaning of their environment.

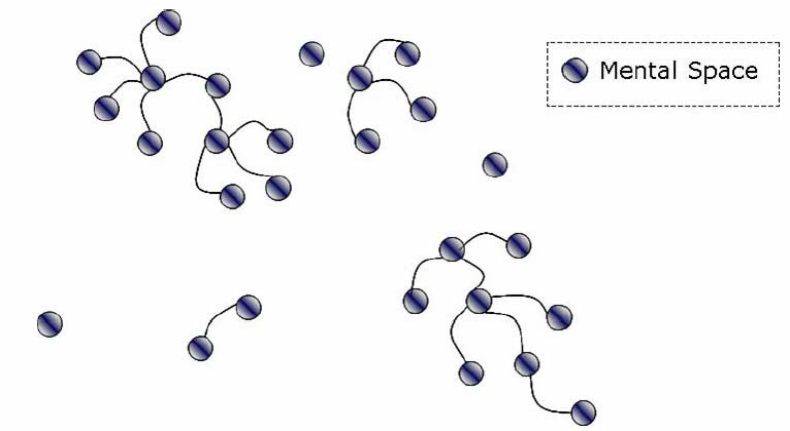

Figure 4. Complex integration networks (From Ref: 21)

A critical aspect of conceptual blending is not the blend but rather the finding of relations (the solid lines) between the mental spaces that leads to the blend. The theory calls these all-important relations "vital relations". The links between input mental spaces, known as "outer-space" links can be compressed into relations, known as "inner-space" relations, inside the blend itself. It is this ability to achieve compression through blending that give humans "global insight, human-scale understanding and new meaning" with efficiency and creativity [22]. Some vital relations identified by the theory are shown in Table 4.

Integration and compression alone is insufficient. Disintegration and decompression, the ability for projections to be made from the blend back onto its disintegrated input spaces, are required as well. The blend has to be connected back to the rest of the network. Human understanding is a matter of activating and connecting compressions and decompressions simultaneously in the entire network [22]. There are multiple possibilities of compression and decompression, relations among mental spaces,

the kinds of projection and emergence. This leads to a large variety of integration networks.

Change	Identity	Time	Space
Cause-Effect	Part-Whole	Representation	Role
Property	Intentionality	Similarity	Uniqueness

Table 4. Vital Relations

F. MULTIAGENT SYSTEM FOR ADVERSARIAL PLAN RECOGNITION

In high-threat situations, tactical decision makers must analyze large volumes of data from external sensors and other sources simultaneously and quickly. This is necessary in order to correctly assess the enemy intentions and decisions can then be made in within short periods of time. The studies on threat assessment in the domains of naval air defense and surface warfare have revealed that a large number of factors will have to be considered by the decision makers [29] [30]. As the adversary may act singly or in concert, the tactical decision maker must also possess knowledge of a broad array of choices from among the adversary's potential tactical patterns. This problem is exacerbated by information "gaps" due to sensor inadequacies and misinformation subject to enemy deception [23].

The Plan Recognition for Airborne Threats (PRAT) system [23] by Amori can perform adversarial plan recognition for airborne using a multi-agent architecture derived from plan-based natural language understanding. The architecture is comprised of single agents used for reasoning about the intentions of individual adversaries. Each individual agent contains two components, a backward component and a forward component. Track data are stored in "rolling" or dynamic-content data structures in the backward component. The forward component for reasoning uses these data structures for reasoning about the intention of a track and the result is stored in similar data structures as well. As the scenario changes, the track data in the backward component is updated

regularly. The forward component changes its hypotheses about the track dynamically over time as well as new evidence becomes available.

The architecture also contains sets of agents that are grouped together when the tracks they represent are suspected of acting in possible coordinated attacks. Similar to the individual agents, each agent in these groups also contains the same backward and forward components. In this case, the forward component stores the result of reasoning on group behavior among these cooperating agents. The PRAT system is able to perform complicated 3-dimensional and temporal reasoning under real-time requirements. Using a divide-and-conquer strategy, the system blends high volumes of sensor data with agent behavioral characteristics and tactical doctrines in order to infer adversarial plans [23].

G. MULTIAGENT SYSTEM FOR THREAT ASSESSMENT

A different multi-agent architecture for threat assessment, fusing a sense-update-act agent operation paradigm together with elements of cognitive blending theory, was described by Ozkan [21]. A basic Sense-Update-Act agent architecture, proposed by Susanne Barber from the University of Texas, is shown in Figure 5. The basic agent in this architecture is embedded in an environment from which it receives sensory inputs through a sensory pathway. Changes to the state of the environment are achieved through a behavior actuator channel.

The functionality and organization of this architecture was further refined by John Hiles in his project on Integrated Asymmetric Goal Assessment (IAGO) at the Naval Postgraduate School [31]. The expanded architecture subsumes multiple agents within an external environment, shown in Figure 6. There are several possible types of agents in this architecture.

1. Reactive Agents

These are simple agents that act as transducers that translate input data or signals from the environment into control or data signals that are sent back into the environment. They do not retain state information or use sophisticated internal cognitive models for their tasks [31].

2. Cognitive Agents

These agents maintains internal state information and models for their processing. This allows them to act in conjunction to historical data and past conclusions so their behaviors may change over time. These agents are able to formulate goals, incrementally collect information over time in order to prove or refute these goals, and then act according to their results. Their state knowledge can be externalized as well so that other agents, the environments and even humans may understand what these cognitive agents know and why they are behaving in some manner [31].

3. Composite Agents

These are specialized instances of cognitive agents that contain internally other agents. The nested agents do not interact directly with the external environment. Instead the internal environment of the containing agent provides these nested or internal agents with a localized context for data sets and belief maintenance. The internal agents are typically used to maintain more complex state information and sophisticated cognitive models that may include interaction of several internal agents [31].

4. Families of Agents

Agents can be further grouped together into homogenous groups where each member agent perform the same functions, or into heterogeneous groups with many types of member agents. Research into complex adaptive systems using aggregates of agents has shown that these agent groups are able to exhibit synergistic or emergent behaviors. As a result of these collective behaviors, insights into very complex systems can be obtained [31].

Building on this agent architecture and the theory of cognitive blending, an Air Defense Laboratory (ADL) simulation was proposed by Ozkan [21] to model the way an air-defense officer makes threat assessments. This research is also part of the Red Team Intent project which is a multi-agent system for discerning the intentions of any track operating within an area under observation [32].

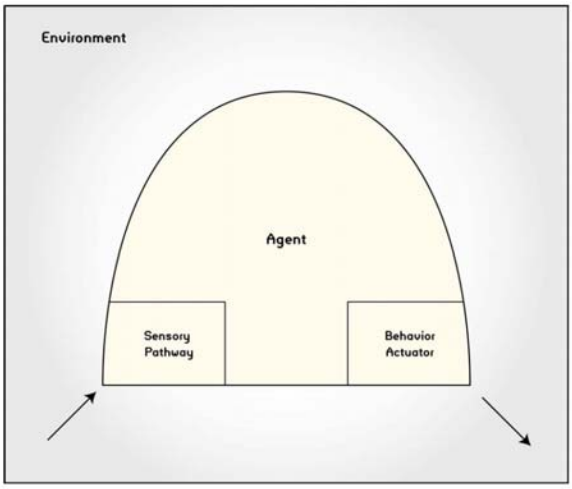

Figure 5. The Sense-Update-Act agent architecture (From Ref: 31)

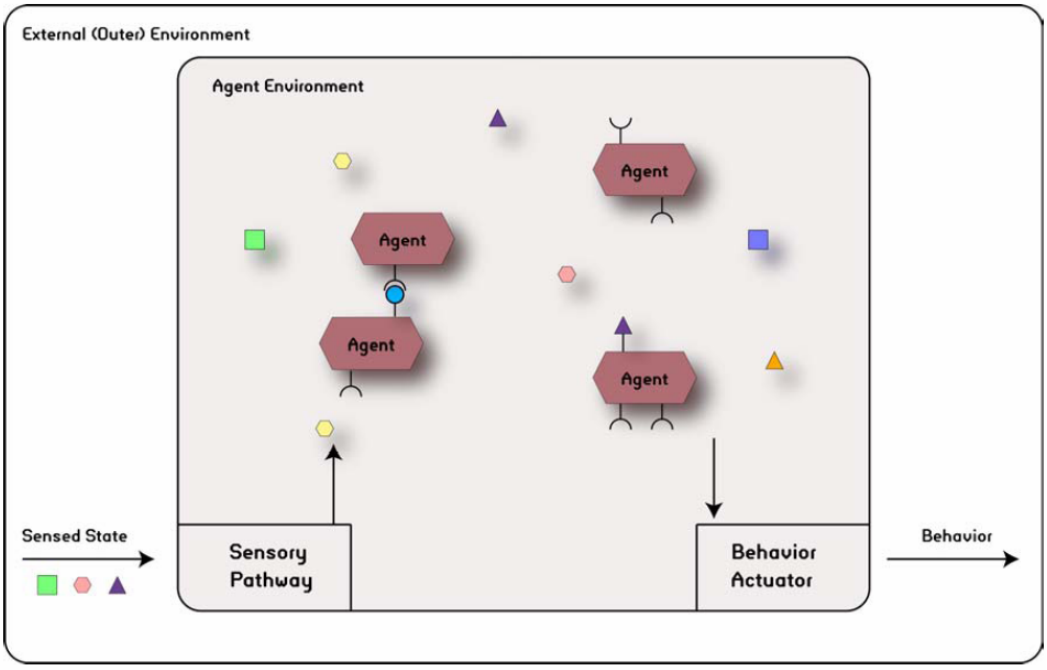

Figure 6. The Generalized Sense-Update-Act agent architecture (From Ref: 31)

The ADL simulation system uses a 3-layer multi-agent architecture shown in Figure 7. The architecture is based on the generalized sense-update-act agent paradigm, to predict the identity of air tracks. In the bottom layer, each track in the simulation has a set of reactive agents, each focused on specific different track features and data. These

reactive agents act like localized sensors that receive information from the external environment and transmit the information to a predictor agent in the next layer above.

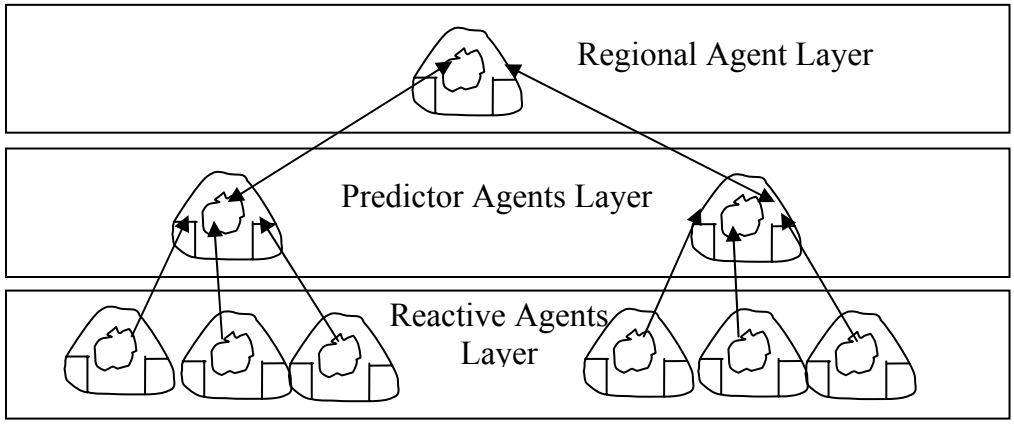

Figure 7. The 3-layer multi-agent architecture of the ADL simulation system

Every predictor agent maintains five competing models for identity prediction: Civilian, Unknown, Friendly, Suspect and Hostile. These cognitive models are constantly updated with new information about the track coming up from the bottom layer. Based on past and current the track data, each model will compute a score that represents the strength of the identity that it represents. At any time, the model with the highest score will be considered the active model and the identity it represents will be the predicted identity for the track.

There is only one regional agent at the topmost layer that is responsible for finding coordinated activities between tracks. This is done by monitoring for regional activities involving more than one track. The ADL simulation is able to find three types of coordinated activity for air tracks:

1. striker with coordinated snooper-support,
2. coordinated detachment involving two tracks turning in concert, and
3. merge activity where two tracks are joining.

Interaction between the predictor and regional agents is bidirectional. When a track is discovered to be involved in one of the three regional coordinated activities, the

regional agent will report this new insight back to the predictor agent. The predictor agent will use this feedback to reinforce one or more of its nested identity models.

The ADL simulation uses a combination of conceptual blending and evidence weighting algorithm in order to establish a track's identity. Fusing track features and information is achieved by blending operations, similar to other methods of identity estimation involving pattern-recognition based on clustering algorithms, neural networks, or decision-based techniques like Bayesian inference or weighted-decision techniques. An example of how a coordinated merge activity is shown in Figure 8. A coordinated merge activity can be detected by:

1. mapping the data of two tracks in the input mental spaces with vital relations (also known as *Composition*),

2. projection of the relevant data from the input space onto a structure or pattern of a merge operation which is specified in a generic space (also known as *Completion*), and

3. the compression of the generic structure from the generic space and the specific track information and associated vital relations into a blend which represents a merge activity between the two tracks.

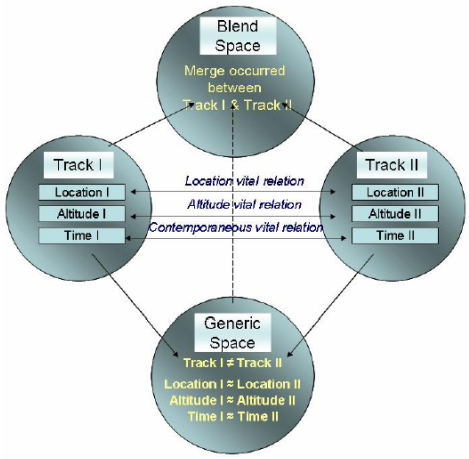

Figure 8. Merge Detector Blending Operation (From Ref: 21)

The identity models are represented as groups of nodes in the resultant integration network that is formed by the blending operations. The nodes are then weighted based on the Bayesian inference process suggested by Liebhaber's research in threat assessment [21].

H. CONCLUSION

Several multi-agent models for threat assessment were presented. These systems apply some of the cognitive processes that human military experts use for making decisions under stress. Among these systems is a multi-agent system (MAS) that uses conceptual blending. This novel theory of human understanding has been applied successfully in the domain of air threat assessment. The idea of using a MAS for threat assessment will be applied in the domain of surface contact threat assessment. The MAS will use threat level cues for surface warfare to determine the intent of surface contacts. The design of the MAS will be presented in detail in Chapter III.

III. DESIGN OF THE MULTI-AGENT SYSTEM

A. INTRODUCTION

Thus far we have described a compound multi-agent system (MAS) designed for surface threat intent identification. Each surface contact is represented by a track agent which has a nested MAS that continuously processes incoming information about the contact in order to discover the likely intent of the contact. Each nested MAS uses track data and information of key maritime traffic elements such as Traffic Separation Schemes (TSS) and Area-To-Be-Avoided (ATBA) zones. The MAS also incorporates the threat assessment cues that experienced surface warfare personnel use for surface threat assessment [30]. This chapter describes the layered hierarchy of agents inside the MAS: the different types of agents and their roles, how the agents interact and coordinate to generate blends, and how weighted scoring strategies are used to deduce the intent of a track.

B. THE CMAS LIBRARY

The communication and coordination among many different agents in the nested MAS is achieved using the Connector-based Multi-agent Simulation Library (CMAS) developed by John Hiles and his team at the Naval Postgraduate School [31]. The CMAS library has been used in projects such as the US Army game "Soldiers" and Project IAGO (Integrated Asymmetric Goal Assessment) [31].

The basic elements for agent communication and control within the CMAS framework are connectors. The agents use these connectors to externalize portions of their internal states into the multi-agent environment. Connectors are like plugs and receptacles that can be extended or retracted as shown in Figure 9. Agent 1 can signal to the external multi-agent environment two pieces of its internal information by extending two connectors known as stimulus connectors. Meanwhile Agent 2 in the same environment has registered its interest in receiving two pieces of the same information by extending two response connectors that queries the environment for the information.

Signaling and coordination between the two agents occurs when there are matching pairs of plug-receptacle connectors and the connectors get connected.

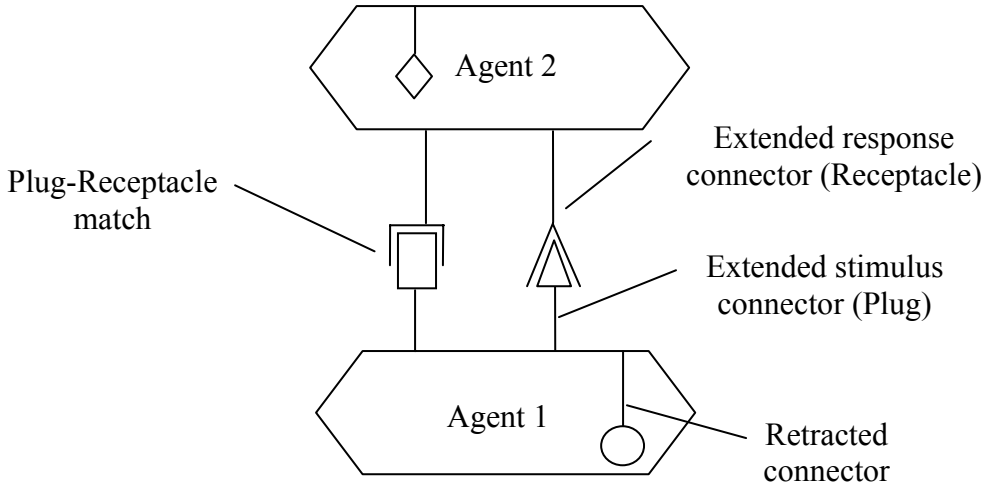

Figure 9. Connectors for agent communication and coordination

The CMAS library also uses the concept of tickets as a mechanism for encoding procedural instructions for agents as well as to provide an internal data organizing system. There are two types of tickets – data tickets are used to organize and assess the completion status of hierarchical structures, and procedural tickets are used to generate appropriate agent behavior in response to the state of another agent's tickets and connectors. More information about the use of tickets can be found in the "CMAS Users Guide" [31]. Currently, the MAS only use connectors for agent communication and coordination. Data structures and agent behavior are currently implemented natively in the agents without the use of tickets.

C. THE MULTI-LAYERED ANATOMY OF A TRACK AGENT

Every surface contact in the MAS is represented by a corresponding track agent. Inside every track agent is another nested MAS so the overall system can be considered a compound MAS. The layered agent architecture nested inside every Track agent is shown in Figure 10. There are four layers of agents working in tandem. Information

propagates upwards from the lower layers. The information may be processed further to infer more information about a track and the new information also propagated upwards. Finally, the topmost layer consists of intent agents that decide the current intent of a track.

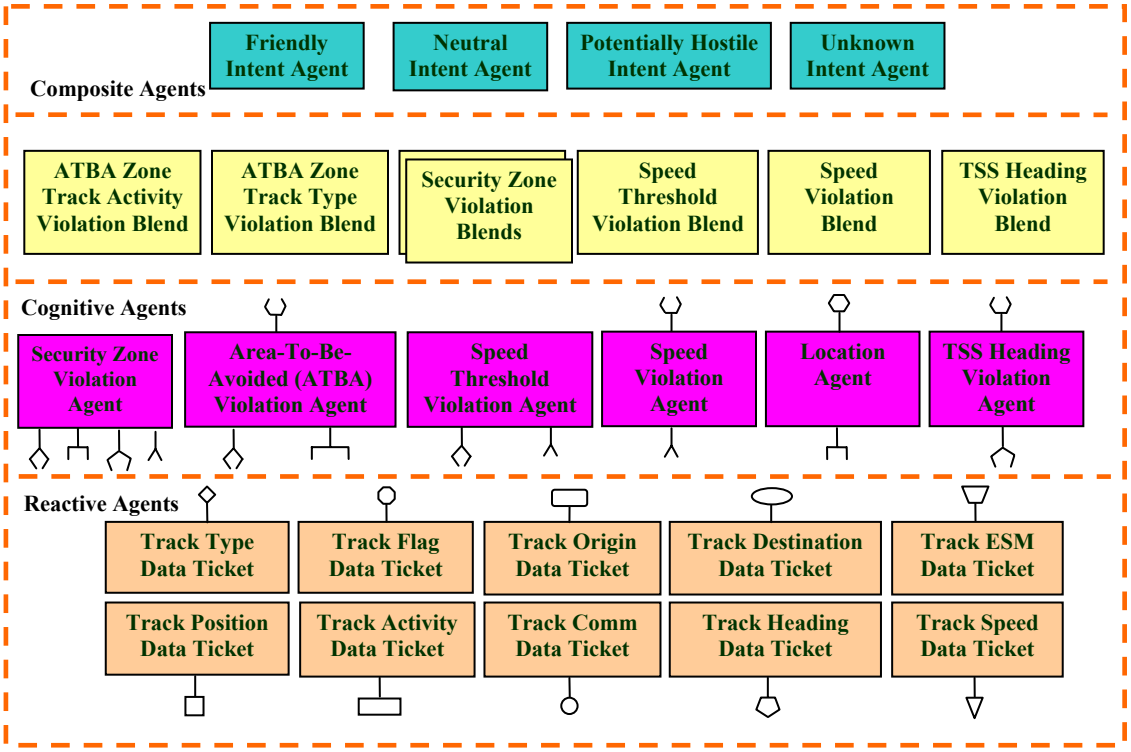

Figure 10. The nested MAS inside each Track agent

1. The Layer of Track Data Agents

The lowest level consists of purely reactive data agents, also known as data tickets. Their primary function is to act like an interface to the outside world and to carry information from the outside world into the internal environment of the MAS environment where all the other agents reside. The information provided by the layer of track data agents will be used by the cognitive agent layer above. Table 5 shows the details of the track data that are currently used in the MAS.

Data Name	Description
Track Type	The type of track. The possible values are: 1. Unknown 2. Police Coast Guard (PCG) 3. Military 4. Cruise Liner 5. Leisure 6. Tanker 7. Fishing 8. Oiler
Position	The current position of the track in GEO Lat and GEO Long.
Track Flag	The flag of the track. The possible values are: 1. Unknown 2. Own 3. Friend 4. Neutral 5. Hostile
Track Destination	Destination of the track. This is the name of the destination that the track is going to.
Track Heading	The current heading of the track in degrees.
Track Speed	The current speed of the track in knots.
Track Comm	The existence of voice communication with the track. The possible values are: 1. Unknown 2. Yes 3. No
Track Activity	The current activity of the track. The possible values are: 1. Unknown 2. Patrol 3. Cruise 4. Fishing

Track Origin	The point of origin of the track. The possible values are: 1. Unknown 2. Own 3. Friend 4. Neutral 5. Hostile
Track ESM	The presence of Electronic Support Measures (ESM)/Radar Emitter. The possible values are: 1. Unknown 2. None 3. I-Band 4. X-Band 5. Others

Table 5. Track data used by the MAS

2. The Layer of Cognitive Agents

The cognitive agents use the information provided by the lower level of data agents to make inferences to discover if a track is

1. in a special area like a traffic separation scheme (TSS) or restricted area, and
2. violating any rules or traveling in a dangerous or atypical manner.

a. The Location Agent

The Location Agent uses the track's current position to decide whether the track is inside a special area e.g. in a TSS, or inside a restricted zone where rules on track type, speed, activity and other track attributes may apply. This is achieved by investigating user-defined locations and sizes of the Traffic Separation Schemes (TSS) and restricted zones.

b. TSS Heading Violation Agent

A Traffic Separation Scheme (TSS) is a sea-lane with a predefined traffic direction that has been designated by a Vessel Traffic Service operating in a harbor. Under Rule 10 of the International Navigation Rules formalized by the International Maritime Organization (IMO) at the Convention on the International Regulations for Preventing Collisions at Sea, 1972, (72COLREGS), "a track using a traffic separation scheme shall proceed in the appropriate traffic lane in the general direction of traffic flow for that lane" [34]. If the MAS found a track violating the traffic direction of a TSS, a TSS heading violation occurs.

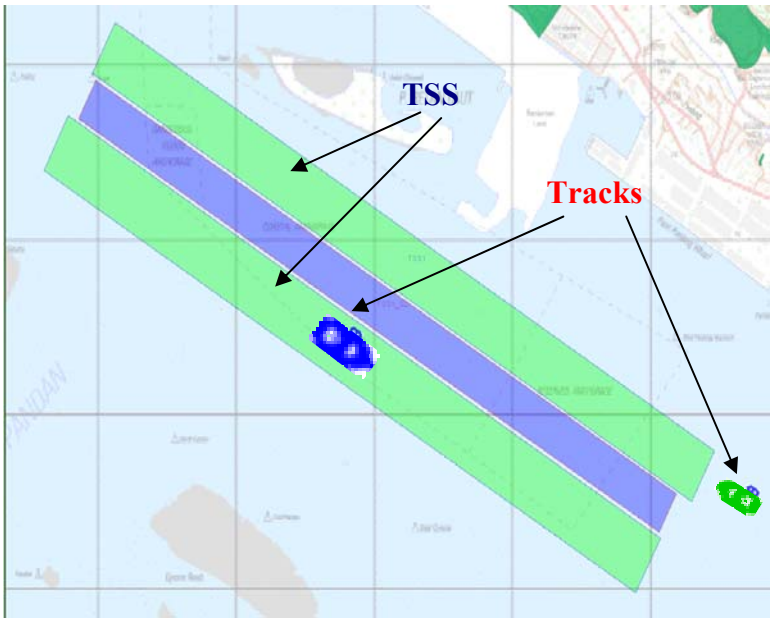

Figure 11. A Traffic Separation Scheme (TSS)

c. Speed Violation Agent

Rule 6 of the 72COLREGS states that "every vessel shall at all times proceed at a safe speed so that she can take proper and effective action to avoid collision and be stopped within a distance appropriate to the prevailing circumstances and conditions" [34]. A TSS may also have minimum and maximum speed limits that tracks traveling inside a TSS is expected to comply for prudent seamanship. There can also be minimum and maximum speed limits defined for other designated areas e.g. in a harbor

or in fishing areas in the surrounding waterways, where there are high traffic density. A speed violation occurs when a track fails to comply with the speed limits defined in these areas.

d. Speed Threshold Violation Agent

Rule 6 of the 72COLREGS also states that safe speed is also related to the "maneuverability of the vessel with special reference to stopping distance and turning ability" [34]. Besides predefined speed limits for designated areas, the MAS also checks for speed limits defined for different track types. Different track types can have different maximum speed limit thresholds that are considered normal for the track types. If a track is found to be traveling at an atypically excessive speed based on its track type, the system detects a speed threshold violation.

e. Security Zone Violation Agent

Cruise-liners, tankers, ferries, military craft are examples of High Value Units (HVUs). The MAS will help monitor for potentially hostile intent against these HVUs by encircling them with user-defined security zones [35] [36] as shown in Figure 12. Only certain types of pre-defined tracks e.g. police coast guards (PCGs) may be allowed within these security zones. Each security zone is associated with an alert time which can be considered as a user-defined time required by a HVU to respond when another track encroaches into one of its security zones.

As HVUs move, the MAS continually monitors the CPA (Closest Point of Approach) and TCPA (Time to CPA) of other tracks around it. When an unauthorized track has a CPA that falls within a security zone of a HVU and its TCPA is less than the Alert Time defined for the zone, a security zone violation occurs, as shown in Figure 13. Security zones can also be defined for static HVUs e.g. military installations, oil refineries, ferry terminals that may be located near or on the coast. Similarly, a security zone violation occurs when an unauthorized track has a CPA inside a security zone and its corresponding TCPA is less than the Alert Time threshold for the security zone.

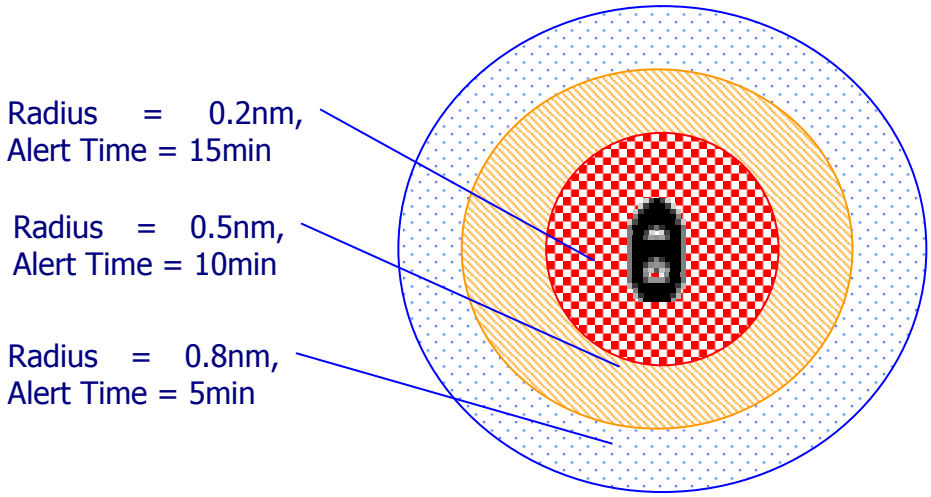

Figure 12. Security Zones around a HVU

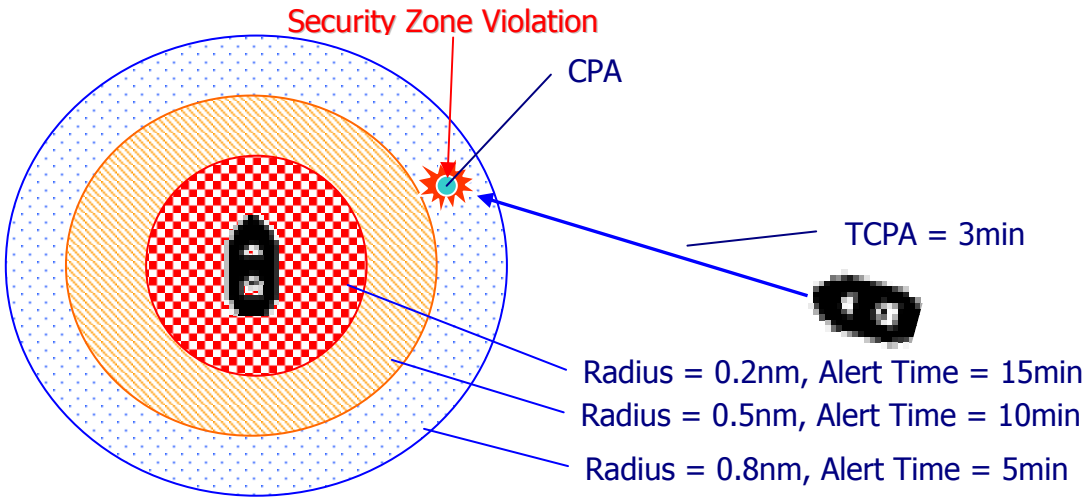

Figure 13. Security Zone Violation

f. Area-To-Be-Avoided Violation Agent

An ATBA is defined by the IMO as "an area that all ships or certain classes of ships should avoid because navigation is particularly hazardous or it is exceptionally important to avoid casualties within the area [37]." Areas-To-Be-Avoided (ATBAs) may also be defined near restricted areas e.g. oil refineries and military installations. Only certain types of tracks and track activities may be allowed within these ATBAs. The MAS detects an ATBA violation when an unauthorized track intrudes into an ATBA.

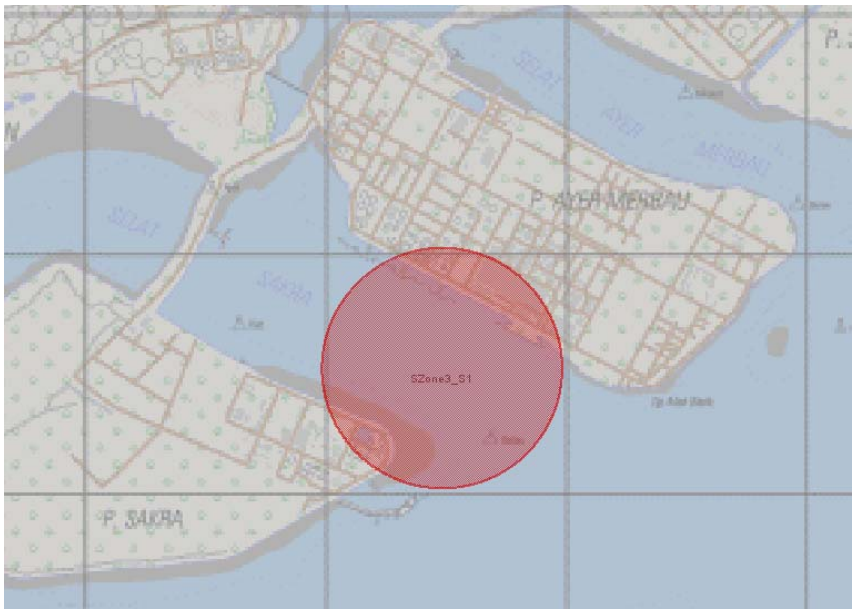

Figure 14. An Area-To-Be-Avoided

3. Track Violations and Cognitive Blending Operations

A track violation is discovered by a Violation agent through the integration of track data, rules and regulations of the VTS and other user-defined information using conceptual blending operations. A track's CPA and TCPA from an input mental space for a track is connected, through Distance and Time Vital Relations, to another input mental space representing the definition of a security zone and the corresponding alert time around a HVU, as shown in Figure 15. Note that the input mental space of a track contains other information besides CPA and TCPA.

The generic space is required to guide the selective projection of the relevant information into the blended space. In this case, the generic space is provided by the Violation agent. It contains the rules regarding the conditions that constitute a security zone violation.

The CMAS library provides connector-based (receptacle-plug) agent communication to the agents in the MAS environment. The Security Zone Violation agent extends queries (receptacles) into the MAS environment for specific track data that is specified in the generic space, as shown in Figure 16. The relevant track data agents or data tickets respond to the queries, if their connectors are extended, by plugging their

connectors into the corresponding receptacles and transfer the required information to the Violation agent. Based on the track's current position, speed and heading, its CPA and TCPA to surrounding High Value Units (HVUs) are calculated by the Violation agent.

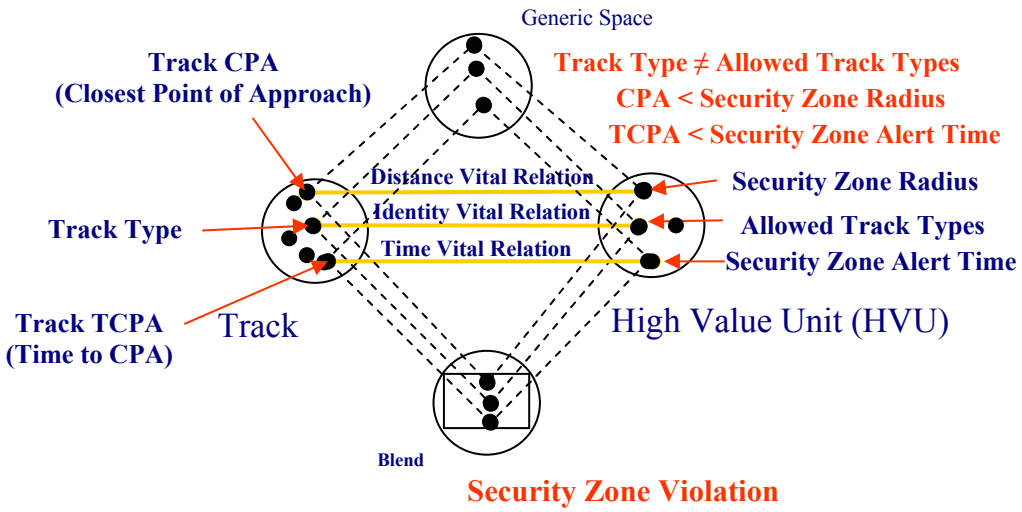

Figure 15. An example of a Security Zone Violation blend

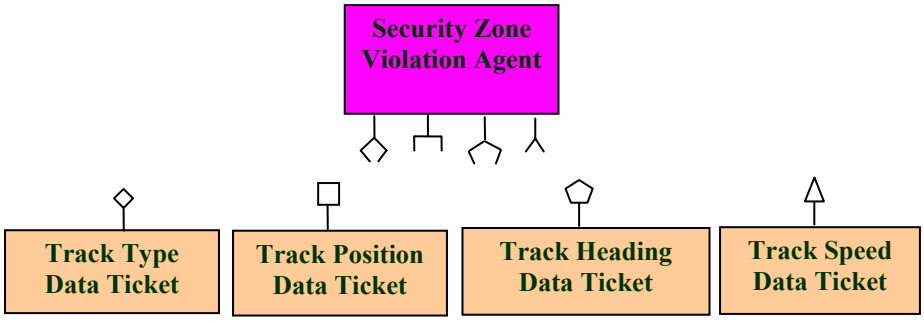

Figure 16. Using connectors to query for track data

Finally, a blended space representing a security zone violation is formed by the inference based, in this case the computed CPA and TCPA, on information projected from the input mental spaces. The Security Zone Violation blend is spawned by the Security Zone Violation Agent. The blend can be considered a simple reactive agent. Another example of how cognitive blending operation is used to detect an ATBA Zone Track Activity Violation is shown in Figure 17. This case generates an ATBA

Zone Track Activity Violation blend. These violation blends, together with other violation blends, forms an intermediate layer of simple reactive agents that work with the topmost layer of intent agents.

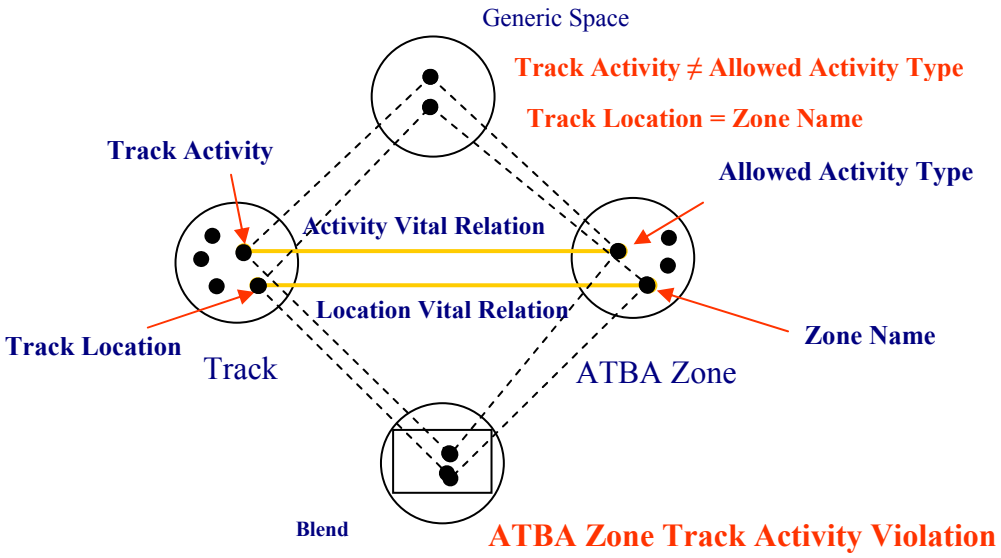

Figure 17. Example of an ATBA Zone Track Activity Violation blend

D. THE ANATOMY OF AN INTENT AGENT

The top layer of agents of the nested MAS environment inside a track agent comprise of Intent agents. There are four Intent agents: Friendly, Neutral, Potentially Hostile, and Unknown. Each of these Intent agents uses a family of "helper" agents as shown in Figure 18. The intent agents use information provided by agents from the lower layers. This information includes track location, violations, origin, flag, and existence of voice communication with the track, among other indicators.

The family of weighting agents is responsible for obtaining information, using connectors provided by the CMAS library, from the lower layers of data agents and blends. Note that there is a one-to-one relationship between a weighting agent and a data agent or blend, as shown in Figure 19. The weighting agents then forward information received to a Weighting Strategy. The Weighting Strategy defines the intent model i.e. Friendly, Neutral, Potentially Hostile, Unknown, that the Intent agent represents. The Weighting Strategy assigns user-defined weights to each piece of track information that

the Weighting agents receive, similar to the Threat Level Change Ratings scheme identified from the study in surface warfare threat assessment process by Liebhaber and Feher [30].

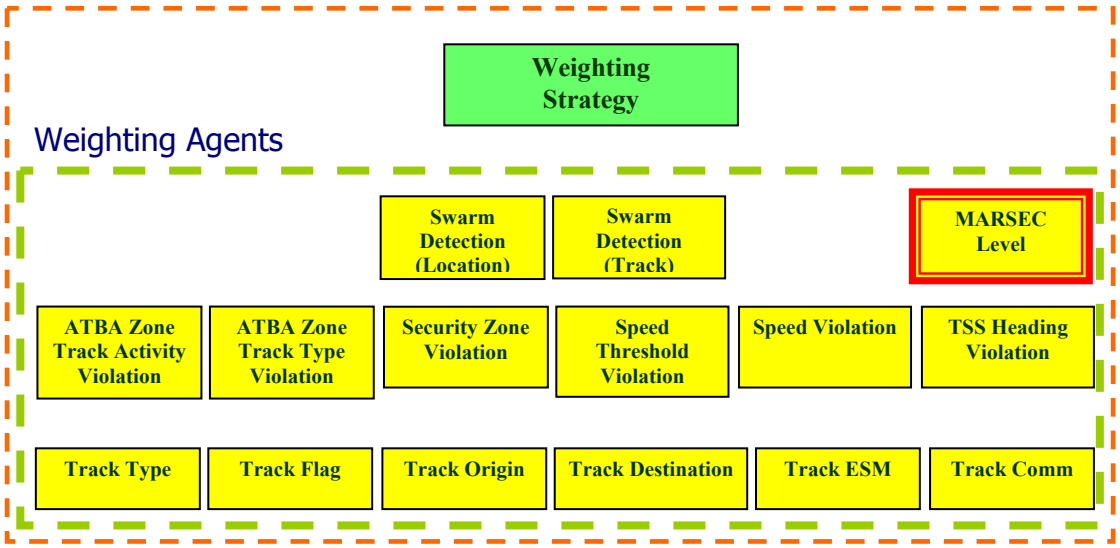

Figure 18. The nested MAS inside each Intent agent

The Weighting Strategy associated with each Intent model has a unique set of weights. When new information about a track is available from the Weighting agents, all the Weighting Strategies compute a revised score using its own set of weights for the new information. Effectively, the Intent models compete, and the one with the highest score represents the current intent of the track.

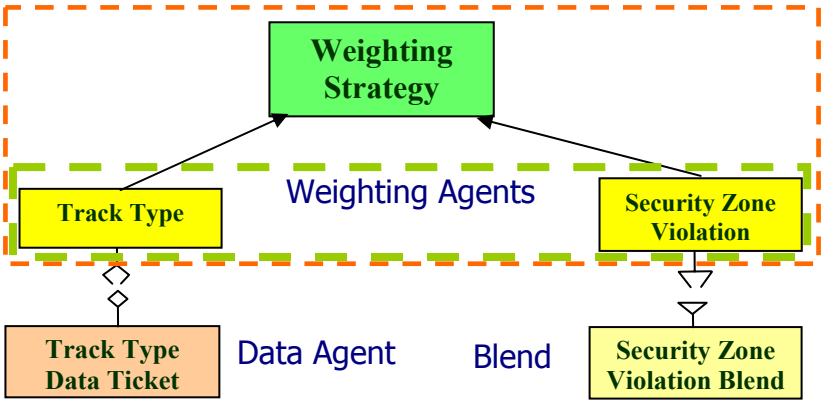

Figure 19. Interaction between the weighting agents and other agents

E. THE REGIONAL AGENT LAYER

Looking from outside the MAS environment of a track agent, a track agent appears as a single agent that exists in another external MAS environment. In this external MAS environment, there is a layer of regional agents that monitor the behavior of all the track agents, as shown in Figure 20. Currently, two types of regional agents detect coordinated behavior that resembles an impending swarm or a "wolf-pack" (a common maritime terrorist tactic [10]) attack on another track or against a restricted location such as an oil refinery or a military installation. Swarm Detection agents compare the Security Zone Violation blends generated by the track agents. If there are several similar violation blends by different tracks against another track or location, the regional agent produces a Swarm Detection blend, shown in Figure 21. This blend signals the weighting strategies of the track agents suspected of participating in a coordinated attack. The weighting strategies then use the new information to revise the intent of the track agents involved in the coordinated attack.

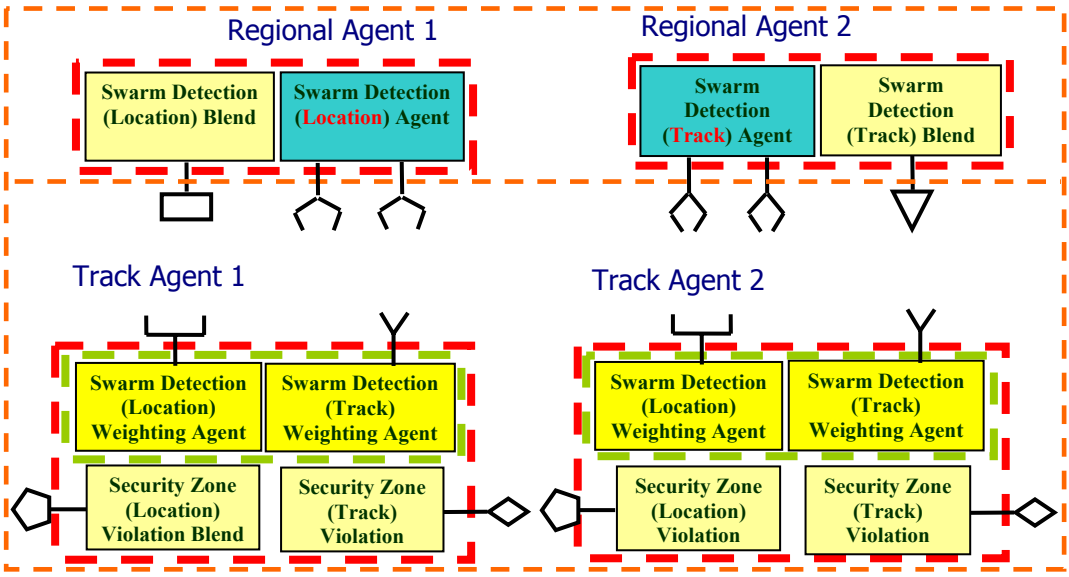

Figure 20. MAS environment of regional and track agents

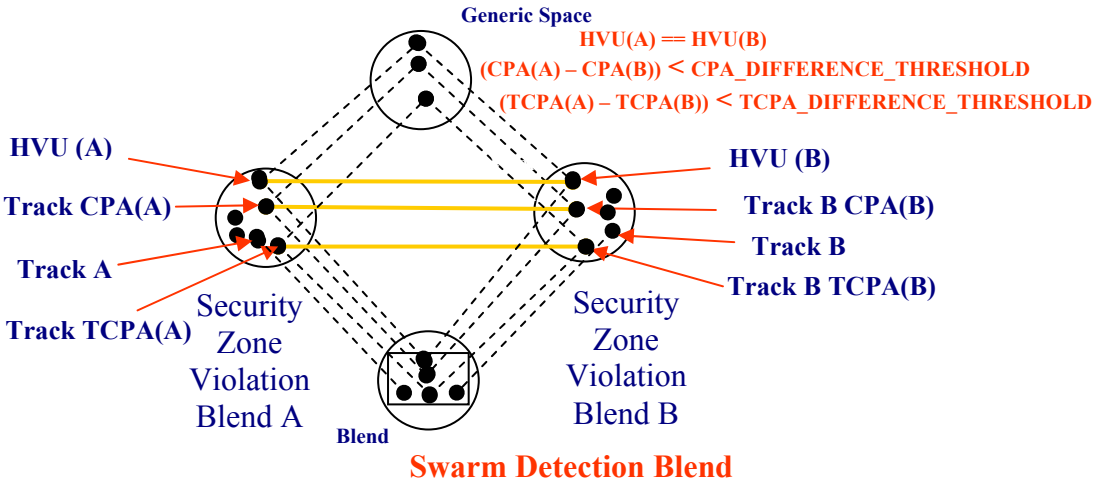

Figure 21. Example of an Swarm Detection Blend

F. THE USE OF REGIONAL INTELLIGENCE

The Department of Homeland Security in the United States has developed the Homeland Security Advisory System (HSAS) to inform local decision makers of threat condition in the country. The higher the HSAS threat level the greater the risk of terrorist attacks. The US Coast Guard (USCG) has enacted a similar threat advisory system [38]. The USCG sets Maritime Security Levels (MARSEC) that corresponds to the HSAS threat conditions. The USCG MARSEC levels are part of an international maritime

protective system [38]. Table 6 shows the HSAS threat conditions and the corresponding MARSEC levels.

Threat Level	Homeland Security Advisory System (HSAS) Threat Conditions	Corresponding Coast Guard MARSEC Levels
Low	Green	MARSEC 1
Guarded	Blue	
Elevated	Yellow	
High	Orange	MARSEC 2
Severe	Red	MARSEC 3

Table 6. HSAS threat conditions and the corresponding MARSEC levels

The MAS also supports a similar 5-level system. By defining a threat level for the MAS, a MARSEC weighting agent inside every track agent heightens or lowers the alertness of the system by causing the weighting strategies to apply appropriate biases to the intent agents.

G. CONCLUSION

The compound MAS design, discussed in this chapter, enables computation of track intent. Inside the compound MAS, there are several families of agents working in tandem. Track data agents extract data from the external world and make the data available inside the MAS environment. Cognitive agents then process and blend the data. Revised track information or blends representing track violations are then relayed upwards into a weighting strategy that exists inside every Intent agent via a layer of weighting agents. The different strategies then use their respective sets of weights to compute a score for the intent model that they represent. The intent model with the highest score represents the current intent of the track.

For verification purposes, the compound MAS is integrated into a mock VTS-C2 simulation system, enabling assessment of various scenarios incorporating hostility that

may exist in a harbor or surrounding waterways. The intent models are evaluated for their effectiveness and the results of the tests will be presented in the following chapter.

IV. VERIFICATION, VALIDATION, AND EXPERIMENTATION

A. INTRODUCTION

To test its effectiveness, the compound MAS, described in Chapter Three, was integrated into a mock VTS-C2 system. This chapter presents the VTS-C2 system with several scenarios involving many tracks, some exhibiting potentially hostile intent, in an effort to validate the MAS on its performance in these scenarios as observed by maritime domain experts.

B. THE VTS-C2 MAS

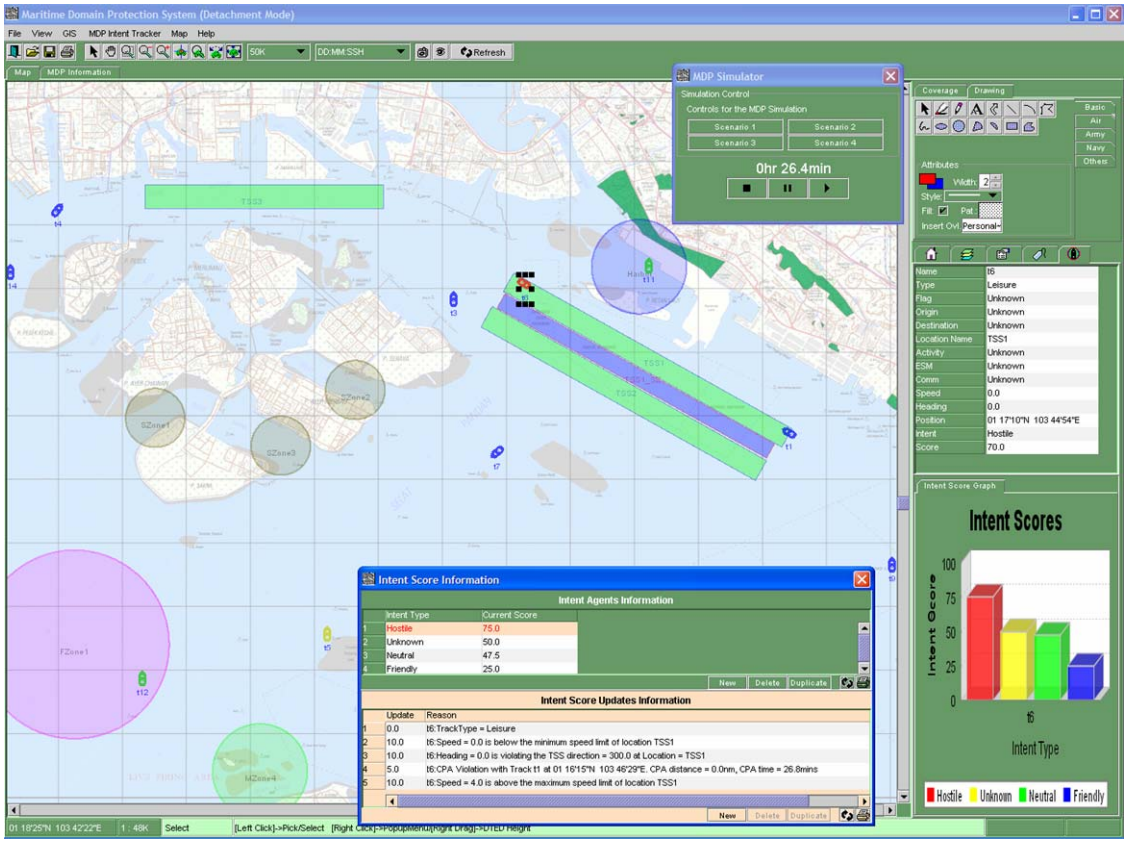

Figure 22. The VTS-C2 MAS

Java-based, the VTS-C2 system supports display of georectified maps, tactical overlays and symbol drawing, and graphical and tabular information displays of C2

information. The system also shows the graphic tracks representing surface contacts, together with traffic separation schemes and restricted areas that are defined in the area of interest. The graphic tracks are colored according to the current intent of the surface contacts. A screen snapshot of the mock VTS-C2 with the integrated MAS is shown in Figure 22.

The compound MAS is the heart of the entire system. It uses information on speed limits, security zone definitions, ATBA definitions, TSS definitions and the current MARSEC level setting. This information is pre-defined in the system using several setup information tables. One such table for defining the security zones around HVUs is shown in Figure 24. The system architecture of the mock VTS-C2 MAS is shown in Figure 23.

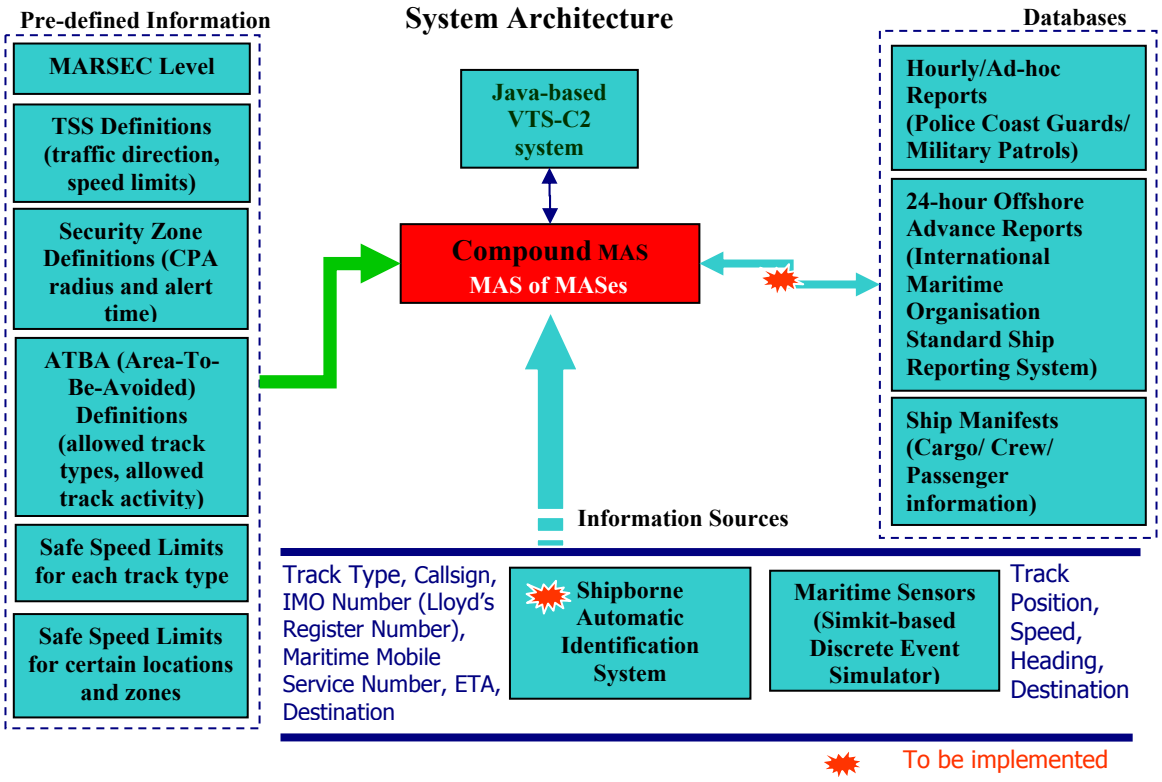

Figure 23. The system architecture of the VTS-C2 system

The system connects to external information sources such as the ship-borne Automatic Identification System (AIS) for track information such as track type, track flag, origin, and destination. The system also uses near real-time information about the surface contacts from maritime sensors. Such information includes track position, speed, and heading.

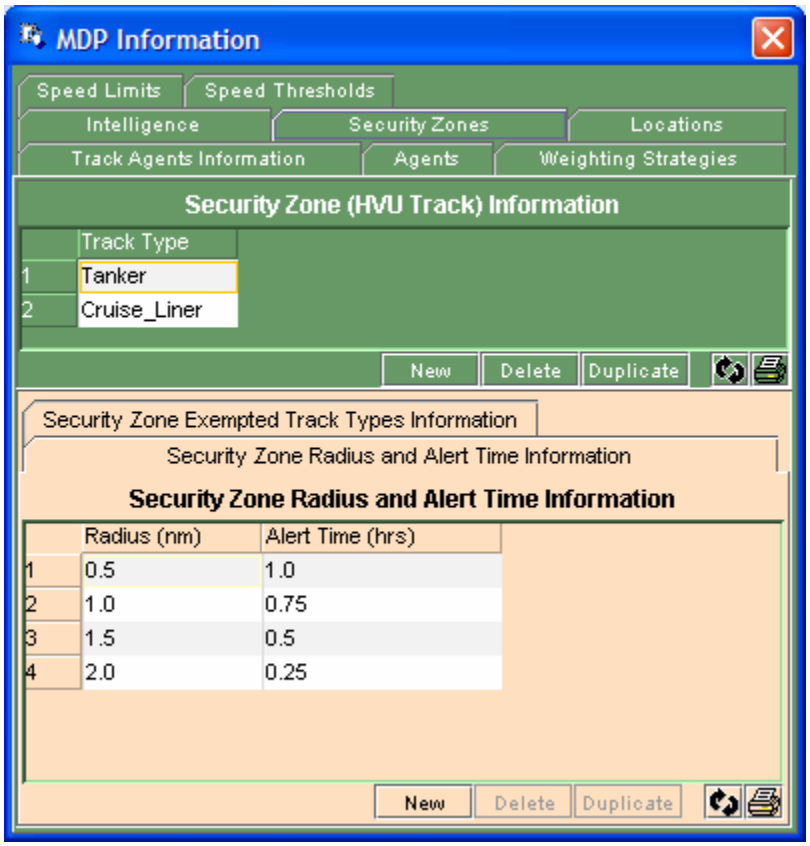

Figure 24. Pre-defined security zone information setup screen

The user can also specify the weight used by the various weighting strategies using one of several weight tables shown in Figure 25. This weight tables also include the bias settings, based on the MARSEC level setting, which the weighting strategies apply on the weights. The values of the weights and biases underlie the weighted scores computed by the competing intent models and therefore predicate the deduced intent of the surface contacts.

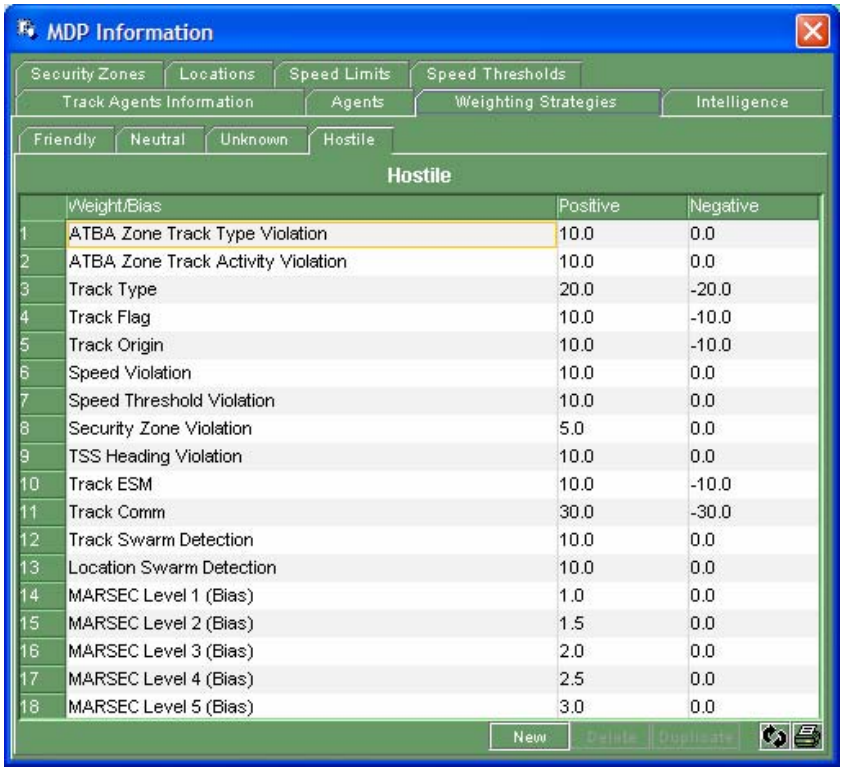

Figure 25. Weights and biases setup screen

It is also possible to set additional agent threshold parameters that the cognitive agents use to detect security zone violations and coordinated attacks, as shown in Figure 26. This allows for some fine-tuning on the frequency and quantity of the violation blends produced by the cognitive agents. The MAS reports computed intents of surface contacts through intent score graphs, shown in Figure 27. The user is also able to get more information on how the scores are computed through a corresponding set of tables shown in Figure 28. The top table shows aggregated weighted scores of the intent models within track agents representing each surface contact and the bottom table shows the breakdown of the aggregate scores into score updates and the reasons for the updates. These detailed breakdowns represent important decompressions of integration networks comprising of information spaces of different entities (tracks, TSSes, ATBAs, security zones) and blends produced by the cognitive agents. This feature of the MAS helps the human understand how track intent is deduced by the system.

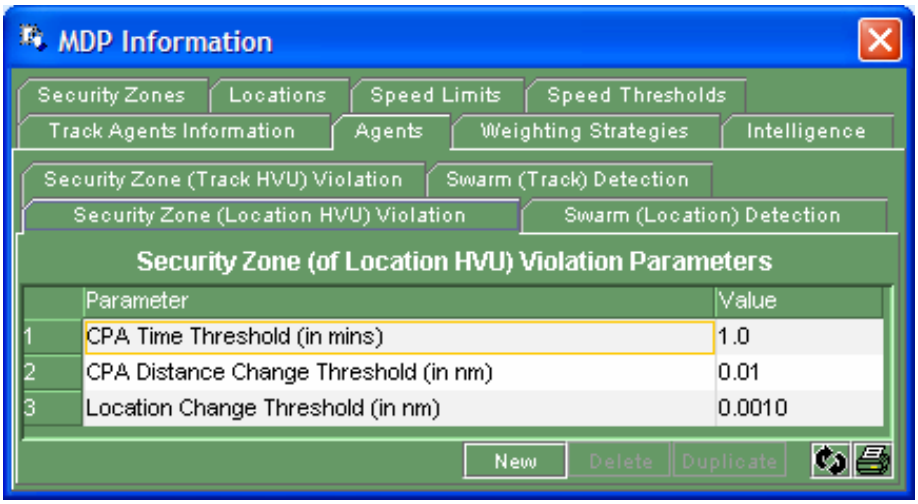

Figure 26. Agent threshold parameters setup screen

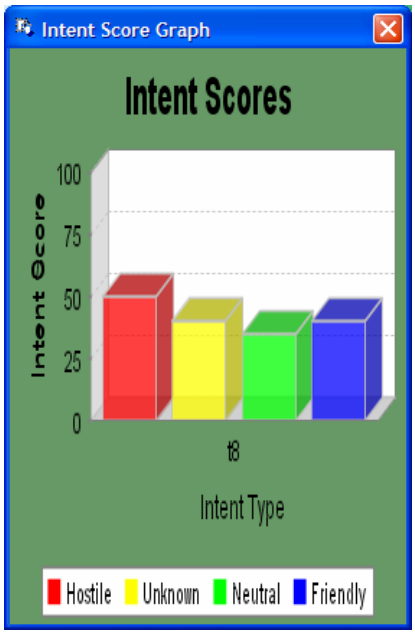

Figure 27. Intent score graph

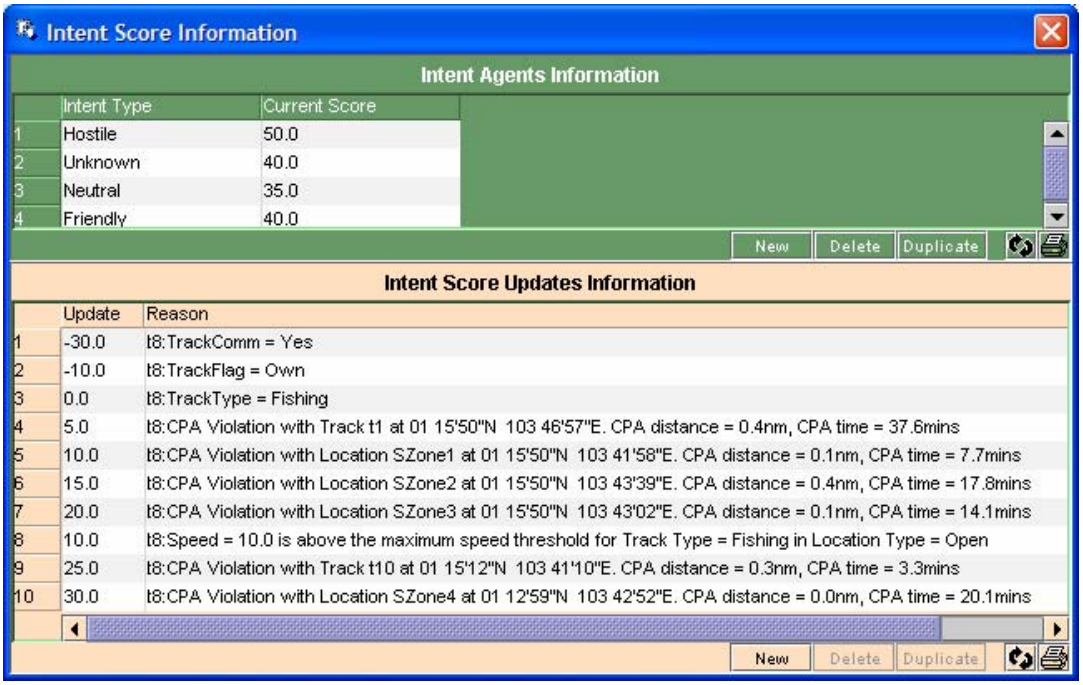

Figure 28. Breakdown of aggregated intent score

The mock VTS-C2 system also has an integrated Discrete Event Simulation (DES) simulator. The DES simulator uses Simkit, a Java-based software package for implementing DES models [39]. In a simulation, every track is represented by a "mover" entity which is an object that can change its position over time. Sensor entities representing each TSS and restricted area are used to detect these moving tracks. If a track is a HVU, it will be attached with security zone sensors, the attributes of which are defined in the HVU security zone information table. As the tracks move, their position is sent to the track agents in the MAS. When a track is detected by any of the sensors, the corresponding track agent is informed that the track has entered the restricted area or security zone represented by the detecting sensor.

C. VALIDATING THE MAS

The value system design approach, a formulation process of a systems engineering effort, provides the basis for a structured and objective evaluation of the MAS. The idea behind this approach is that, by developing objectives and formulating them into objective hierarchies or trees, it is possible for stakeholders of the system to

appraise the objectives by determining the value gained from achieving them [40]. Principle stakeholders include future operators and decision makers of a system. Another important use of the objectives tree is that it helps to define and develop quantifiable objective metrics or criteria that can be used to measure the success in achieving the objectives of the system. An objectives hierarchy for the MAS is shown in Table 7.

	Goal
	Tracking the intent of surface contacts for the purpose of threat identification in busy ports and waterways
	Objectives
1.0	To help the human operator monitor high volume traffic conditions in the port and surrounding waterways
1.1	To monitor multiple surface contacts of all types (PCG, military, cruise liners, leisure, tankers, fishing, oiler)
1.2	To monitor multiple security zones of HVUs (High Value Units) (cruise liners, tankers)
1.3	To monitor restricted areas (oil refineries, cruise center, military installations)
2.0	To monitor that vessels comply with the safety and security rules of the port and waterways
2.1	To check for current track violations
2.1.1	Current incursions into the security zones of HVUs (cruise liners, tankers)
2.1.2	To check for current incursions into restricted areas (cruise center, oil refineries, military installations)
2.1.3	To check for illegal track types/activities in restricted areas
2.1.3.1	Fishing in a non-fishing zone
2.1.3.2	Illegal track type in an Area To Be Avoided (ATBA)
2.1.4	To check for Traffic Separation Scheme (TSS) violations
2.1.4.1	Traveling against traffic direction
2.1.4.2	Stopping in a traffic lane
2.1.4.3	Stopping in a TSS termination zone
2.1.5	To check for speed violations in restricted areas

	Objectives
2.1.5.1	Speed violation in a harbor
2.1.5.2	Speed violations in a traffic lane
2.1.6	To check for Vessel Traffic Service (VTS) violations
2.1.6.1	Collision detection
2.2	To check for future track violations
2.2.1	To check for future incursions into the security zones of HVUs (cruise liners, tankers) using Closest Point of Approach (CPA) and Time to CPA
2.2.2	To check for future incursions into restricted areas (cruise center, oil refineries, military installations)
3.0	To help the decision maker identify suspicious or potentially hostile surface contacts
3.1	To find atypical track behaviors
3.1.1	To check for excessive speed based on track types (fishing, leisure)
3.1.2	To check for excessive number of track violations
3.1.3	To detect participation in coordinated attacks
3.1.3.1	To detect coordinated attack (swarm/"wolf-pack") on a HVU/restricted area
3.2	To determine threat level posed by surface contact
3.2.1	To perform surface threat assessment based on track's attributes e.g. platform, flag, origin, ESM
3.2.1.1	Threat assessment based on Track Type
3.2.1.2	Threat assessment based on Track Flag
3.2.1.3	Threat assessment based on Track Origin
3.2.1.4	Threat assessment based on Track Destination
3.2.1.5	Threat assessment based on Track ESM (Unknown, No emitter, I-Band, X-Band, Others)
3.2.1.6	Threat assessment based on Voice Communication with Track(Yes, No)
3.3	To adapt to the needs of the decision maker
3.3.1	To provide user-defined biases (weights)
3.3.2	To incorporate regional intelligence (5 x MARSEC levels) biases

Table 7. Objectives hierarchy of the MAS

Four validation sessions with four groups of surface warfare and naval officers from the Republic of Singapore Navy and US Navy indicated the impressions these operators and decision makers held for the MAS. Their experiences summed over more than 100 years of harbor security, at-sea and patrol experience between them. Each session featured a brief on the features of the MAS and the mock VTS-C2 system. Next, the participants observed several DES simulations on scenarios involving the port of Singapore and the surrounding waterways. Each scenario featured multiple surface contacts of different types, moving in an area populated with traffic separation schemes and restricted areas and depicted different kinds of hostilities that may exist. The participants received no details in advance.

As the simulations progressed, the participants observed how the MAS determine the intent of the surface contacts. An example of a scenario on a TSS violation and impending collision between a leisure craft and a cruise liner is shown in Figure 29. Another example of a scenario on a coordinated attack on an oil refinery is shown in Figure 30. At the end of each validation session, the participants completed the questionnaire shown in Appendix A.

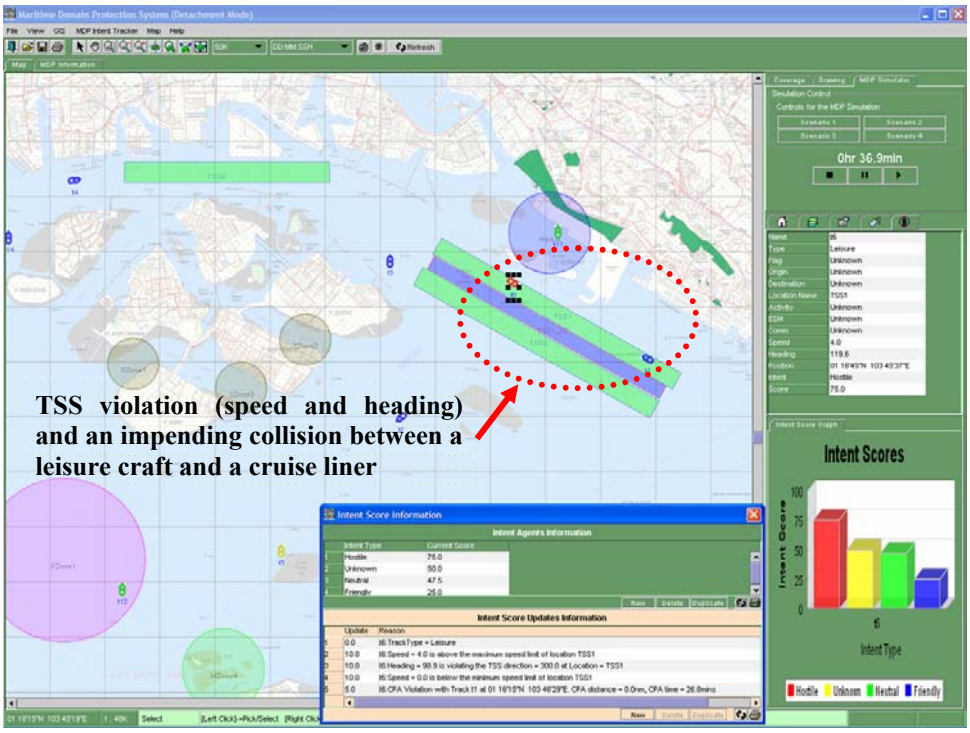

Figure 29. A scenario on an impending collision

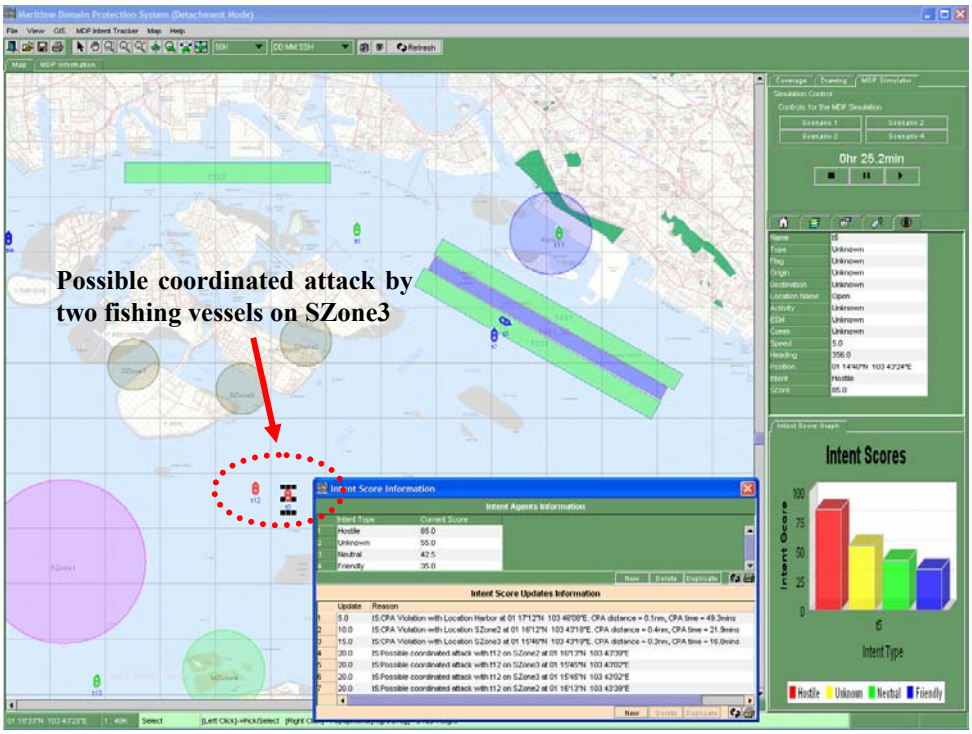

Figure 30. A scenario on a coordinated attack

D. VALIDATION RESULTS

The general consensus among the participants of the validation session is that the MAS is a great advancement in decision aids using compound MAS [49] and can be a very useful system for monitoring movement in busy ports and waterways and being alerted to potentially hostile activity. They agreed on the importance of monitoring all surface contacts, security zones of HVUs and restricted areas. This face validation by potential stakeholders confirmed that the system meets its first main objective of helping the human operator monitor high volume traffic conditions. However, there are also concerns that despite the large amount of information that the system is able to process, there will still be an overwhelming information glut [47]. The human operator also needs to be well trained to use the system effectively [46]. These issues focus on the operator interface more than the processing done by the MAS itself.

With regards to the second main objective of monitoring that vessels comply with the safety and security rules of the port and waterways, the domain experts agreed that

the MAS met this requirement satisfactory. However, the possible number of false alarms that may arise during heavy traffic conditions in the Port of Singapore may be compounded by clutter caused by non-moving surface contacts located in many areas in the congested harbor [44] [45] [48]. However, it is important to note that false alarms are better than no alarms [46]. The domain experts suggest that the weights used by the system have to be calibrated carefully in order to mitigate the number of false alarms.

The domain experts also agree that with respect to the third main objective, the system is a good "proof of concept" that demonstrates how a decision support tool can help the decision maker identify suspicious or potentially hostile surface contacts [44]. It is important to note that system performance is highly dependent on the quality of information and intelligence. This point was made by some domain experts during the validation sessions [46] [47]. The system needs to incorporate specific regional intelligence based on track attributes (e.g. track type, origin and activity) and historical data (e.g. piracy reports).

It is also important to assess the accuracy and reliability of information sources if the MAS was to become an operational system. Although the MAS uses information that may be obtained automatically from the ship-borne Automatic Identification System (AIS), it may also be important to explicitly consider how to interpret the presence or absence of an AIS with respect to the threat level posed by a surface contact [48]. There are also comments raised by the participants from the Republic of Singapore over the semantics of the intent classification labels. Classification of the intent of a surface contact as a "potentially hostile" has certain implications according to their operation doctrine [41] [42] [43]. This issue needs to be considered if the MAS was to be integrated into an existing command and control system.

E. CONCLUSION

The mock VTS-C2 simulation system is built for validating the compound MAS. A DES simulator is also integrated into the VTS-C2 and it is used to simulate various scenarios incorporating hostility that may exist in a harbor or surrounding waterways. Several validation sessions are conducted with domain experts from the both the

Republic of Singapore Navy and the US Navy. The MAS and the intent models are evaluated for their effectiveness in meeting the objectives of the system. Apart from some minor concerns over finer details, results from the validation sessions shows that the MAS is a promising decision support tool that can be used in the maritime security of the Port of Singapore.

After summarizing the work done and findings of the thesis, the next chapter presents some key recommendations on future enhancements to the MAS that are obtained from the domain experts during the validation sessions.

V. RECOMMENDATIONS AND CONCLUSION

A. SUMMARY

Maritime security is especially critical for countries like Singapore, an island nation situated on the southern end of the Malacca Strait, the conduit for 50,000 ships a year, carrying a third of the world's commerce and half of its crude oil [50]. Singapore's economic prosperity is highly dependent on international trade its her busy port, transshipping container terminals, petrochemical complexes, and other high value units located along her coastline. Despite the global decline in the number of reported piracy attacks, the number of attacks in the nearby Malacca Strait has increased with evidence that many have been the work of terrorist organizations from surrounding countries [50]. Singapore's defense minister, Dr Tony Tan has expressed concern these attacks may be practice runs for a terrorist attack. Terrorists may now be learning to be pirates, just as terrorists learned to be pilots for 9/11 [50].

The thesis borrows the ideas and techniques suggested for identifying air threats in the Air Defense Laboratory (ADL) and employ them to identify asymmetric maritime threats in ports and waterways. The four intent models of surface contacts developed for this system - Friend, Neutral, Unknown, and Potentially Hostile, are taken from attributes obtained from VTS manuals, international and inland maritime navigation rules, surface threat assessment requirements reports and known terrorist tactics. Currently these models use the following information to identify hostility and potential:

1. the movement and communication protocols used by vessels registered with the Vessel Traffic Systems (VTS) used in ports and waterways, and

2. a list of surface warfare threat assessment cues that are used by experienced surface warfare officers.

Each surface contact is monitored by a track agent in a compound multi-agent system. Each track agent contains a nested multi-agent system that comprise of the four intent models. The agents communicate and coordinate with a connector-based mechanism provided by the CMAS library. The underlying cognitive mechanism for the intent models is conceptual blending. The theory of conceptual blending is one possible

explanation of how humans are able to think: giving meanings to external information and events, compressing the information into integration networks and eventually learning and gaining experience.

This study used a mock VTS for the Port of Singapore, the waterways and shipping routes around Singapore and included discrete-event simulations of scenarios with maritime hostilities to test the system's ability to identify the intent of multiple simulated surface contacts by blending data and information into integration networks. The intent identification process of a surface contact used by the compound MAS can be obtained through the expansion of the integration networks.

Domain experts provided face validation and constructive feedback. Although the system requires further fine-tuning and verification, the general consensus among the experts is that the MAS has satisfactory address some of the important issues in harbor security and the system has the potential of becoming a useful decision support tool.

B. RECOMMENDATIONS

Before the MAS can be used as a decision support tool, it needs to be verified that the MAS works well against real-world traffic situation in the waters of Singapore. The MAS can also be tested during maritime security drills conducted by the military or Police Coast Guards (PCG). Objective measures for verifying system performance may include the:

1. number of Type I errors (false negatives),
2. number of Type II errors (false positives),
3. time taken by system to identify hostilities compared to a decision maker,
4. amount of lead time the system is able to provide in situations of impending hostilities, and
5. number of factors that the system can process as compared to a human operator.

The MAS can also be further enhanced with the ability to detect more atypical track behaviors or maneuvers such as

1. excessive zig-zag track movement,
2. concealment or evasion from Police Coast Guards (PCG)/Military Patrols,
3. suspicious course changes by monitoring for course/heading of a track in more detail (e.g. in terms of Steady and closing/opening or Turn to closing/opening) to discover if the track is changing its course frequently to match the movement of a nearby HVU,
4. more coordinated activities between tracks e.g. simultaneous attacks on multiple HVUs or restricted areas, and
5. additional VTS violations e.g. failure to submit Offshore Advance reports, wrong/unknown destination.

A noted drawback of the current system is that once a track has been considered as potentially hostile, the system will not modify its designation of the track's intent i.e. the system will neither forgive nor forget the track's behaviors and violations. A future enhancement can have the system use a decaying intent weighting strategy that allows the gradual readjustment of track designations over time [48] [49].

The agents in the current MAS are considered "passive" consumers of information that is fed into the system. It is possible and also important, based on feedback from the validation sessions, that agents can be proactive in automatically searching for more track information i.e. form a paper trail from information sources such as database of ship registration, sail plans, Offshore Advance reports, recent inspections or boardings, cargo/passenger manifests etc. The system can also use context-specific intelligence based on track attributes to identify and focus on a vessel of interest (VOI) [48] [49].

C. CONCLUSION

The primary focus for this thesis is the development of possible surface contact intent models that is useful in threat identification for maritime security. The work done

in this thesis is timely given the increased focus on global maritime surveillance and Maritime Homeland Protection (MHP) of the US [51] and the priorities placed on global maritime intelligence integration and global awareness of civil maritime activities by the Director of Naval Intelligence (DNI) [52]. Preliminary validation results of the four intent models are very encouraging and the models can be refined and be integrated into an existing decision support system or be the basis of a future one for maritime security. Ultimately, it is hoped that the efforts and results of this research can be used to enhance the security of waterways proximal to both the US and Singapore.

LIST OF REFERENCES

1. Maritime and Port Authority of Singapore (MPA), "The Port of Singapore", http://www.mpa.gov.sg/homepage/theport.html, October 2004.

2. Lewis, B., "Background Information Regarding the Port of Singapore and the Port of Savannah", Technical Report, The Logistics Institute, Georgia Tech, and The Logistics Institute – Asia Pacific, National University of Singapore, 2002.

3. Maritime and Port Authority of Singapore, "Achievements and Awards", http://www.mpa.gov.sg/homepage/achieve.html, October 2004.

4. Maritime and Port Authority of Singapore, Port Statistics, http://www.mpa.gov.sg/homepage/portstats.html, October 2004.

5. Maritime and Port Authority of Singapore, "Roles of the MPA", http://www.mpa.gov.sg/homepage/roles.html, October 2004.

6. The Police Coast Guard (PCG), "Background", http://www.spf.gov.sg/about_spf/pcg2, October 2004.

7. The Republic of Singapore Navy (RSN), http://www.mindef.gov.sg/navy, October 2004.

8. Ministry of Defence, Ministry of Home Affairs, Singapore Police Force(MPA), "News Release : Ministerial Visit to the Police Coast Guard and the Republic of Singapore Navy", http://www2.mha.gov.sg/mha/detailed.jsp?artid=393&type=4&root=0&parent=0&cat=0&mode=arc, January 2005.

9. Davis, A., "Piracy in Southeast Asia Shows Signs of Increased Organization", *Jane's Intelligence Review*, June 01, 2004.

10. Rohan, G., Chalk, P., "Terrorist Tactics and Targets", *Counter Terrorism*, chap 3, 2nd ed., Jane's Information Group, October 2002.

11. Rohan, G., "The Asymmetric Threat From Maritime Terrorism", *Jane's Navy International*, 24-29, October 2001.

12. Center for Strategic and International Studies, "Transnational Threats Update", *Transnational Threats Initiative*, Vol. 2, No. 6, March 2004.

13. Englebert, S. E., "IMO Moves to Enhance International Maritime Security", *The Coast Guard Journal of Safety at Sea Proceedings of the Marine Safety Council*, Vol. 60, No. 2, 14 – 18, April – June 2003.

14. Maritime and Port Authority of Singapore (MPA), Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS), Marine Circular to Ship, No. 15 of 2002, August 2003.

15. International Maritime Organization, "Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS)", Resolution A.917 (22), 29 November 2001.

16. Maritime and Port Authority of Singapore (MPA), Revised Performance Standards and Guidance on Provision of Ship Security Alert Systems, http://www.mpa.gov.sg/homepage/ms/mc03-23.htm, Marine Circular to Shipowners, No. 23 of 2003, October 2004.

17. Maritime and Port Authority of Singapore (MPA), Promulgation of Legislation to Effect Special Measures for the Enhancement of Maritime Security, Port Marine Circular to Shipping Community, Harbour Craft Community, Owners and Operators of Port Facilities, No. 12 of 2004, June 2003.

18. Maritime and Port Authority of Singapore (MPA), Continuous Synopsis Record, Shipping Circular to Ship Owners and Ship Managers of Singapore Ships, No. 7 of 2004, March 2004.

19. Maritime and Port Authority of Singapore (MPA), Harbour Craft Security Code and Security Log, Port Marine Circular to Harbour Craft Community and Shipping Community, No. 18 of 2004, June 2004.

20. Singapore Maritime Portal, Navigational Safety, http://www.singaporemaritimeportal.com/worldbusiestport.htm , October 2004.

21. Ozkan, B. E., *Autonomous Agent-Based Simulation of a Model Simulating the Human Air-Threat Assessment Process*, Master's Thesis, Naval Postgraduate School, Monterey, California, March 2004.

22. Gilles, F., Turner, M., *The Way We Think*, Basic Books, New York, 2002.

23. Amori, R. D., "An Adversarial Plan Recognition System for Multi-agent Airborne Threats", *Symposium on Applied Computing* (1992): 500.

24. Orasanu, J., Connolly, T., "The Reinvention of Decision Making", *Decision Making in Action: Models and Methods*, chap 1, 1995.

25. Klein, G. A., Calderwood, R., MacGregor, D., "Critical decision method for eliciting knowledge", *IEEE Systems, Man, and Cybernetics*, Vol. 19, No. 3, 462 – 472, 1989.

26. Klein, G. A., "A Recognition-Primed Decision (RPD) Model of Rapid Decision Making", *Decision Making in Action: Models and Methods*, chap 6, 1995.

27. Klein, G. A., *Sources of Power*, The MIT Press, 1998.

28. Endsley, M. R., "Toward a theory of situation awareness in dynamic systems", *Human Factors*, 37, 32 – 64, 1995.

29. Liebhaber, M. J., Smith, C. A. P., "Naval Air Defense Threat Assessment: Cognitive Factors Model", *Command and Control Research and Technology Symposium* (1999): 2.

30. Liebhaber, M. J., Feher, B. A., "Surface Warfare Threat Assessment: Requirements Definition", Technical Report 1887, SSC San Diego, 2002.

31. "CMAS System Library User's Guide", Revision 1.1, Naval Postgraduate School, November 2004.

32. "Red Team Intent User's Guide", Naval Postgraduate School, November 2004.

33. Department of Homeland Security & United States Coast Guards, "Steering and Sailing Rules - Rule 10 – Traffic Separation Schemes", *Navigation Rules International-Inland*, M16672.2D.

34. Department of Homeland Security & United States Coast Guards, "Steering and Sailing Rules - Rule 6 – Safe Speed", *Navigation Rules International-Inland*, M16672.2D.

35. Department of Homeland Security, United States Coast Guards, "Security and Safety Zone: Protection of Large Passenger Vessels, Puget Sound, WA", *Federal Register*, Vol. 68, No. 61, March 2003.

36. Department of Homeland Security, United States Coast Guards, "Safety Zone: Protection of Tank Ships, Puget Sound, WA", *Federal Register*, Vol. 68, No. 61, March 2003.

37. Department of Commerce, National Oceanic Atmospheric Administration, "Amendments to the Area To Be Avoided Off The Olympic Coast National Marine Sanctuary", *Federal Register*, Vol. 67, No. 229, November 2002.

38. Poulin, S. D., "U.S. Enacts Measure for Maritime Security", *The Coast Guard Journal of Safety at Sea Proceedings of the Marine Safety Council*, Vol. 60, No. 2, pp. 19 – 23, April – June 2003.

39. Buss, A., "Discrete Event Programming with Simkit", *Simulation News Europe*, Vol. 60, Technical Notes, Issue 32/33, 15 – 25, November 2001.

40. Sage, A. P., Armstrong, J. E., *Introduction to Systems Engineering*, John Wiley & Sons, Inc., 2000.

41. Validation session between Yu Chih Hsu, Major RSN and the author, 16 February 2005.

42. Validation session between Pert Chin Ngin, Major RSN and the author, 16 February 2005.

43. Validation session between Amos Teo, Major RSN and the author, 16 February 2005.

44. Validation session between Eng Yee Toh, Major RSN and the author, 17 February 2005.

45. Validation session between Kwang Yong Toh, Major RSN and the author, 17 February 2005.

46. Validation session between W. Westmoreland, Lieutanent USN and the author, 17 February 2005.

47. Validation session between D. Walton, Lieutanent USN and the author, 17 February 2005.

48. Validation session between R. Gottfried, Lieutanent Commander USN and the author, 25 February 2005.

49. Validation session between J. Kline, Captain USN and the author, 25 February 2005.

50. Burnett, J. S., "The Next 9/11 Could Happen at Sea", *The New York Times*, 22 February 2005.

51. CNO Guidance for 2005.

52. DNI Guidance for 2005.

53. Rodeman, C. A., *In Search Of An Operational Doctrine For Maritime Counterterrorism*, Naval War College, Newport, RI, 2003.

54. Sollosi, J. M., "The Automatic Identification System And Port Security", *The Coast Guard Journal of Safety at Sea Proceedings of the Marine Safety Council*, Vol. 60, No. 2, April – June 2003.

55. Northrup, R., Wysock, M., "Standing The Watch", *The Coast Guard Journal of Safety at Sea Proceedings of the Marine Safety Council*, Vol. 56, No. 4, October-December 1999.

APPENDIX. QUESTIONNAIRE FOR VALIDATING THE INTENT MODELS FOR SURFACE CONTACT INTENT TRACKING

Introduction

The purpose of this questionnaire is to validate the intent models developed in the thesis on a multiagent system (MAS) for tracking the intent of surface contacts. The main goal of this MAS is the identification of possible hostilities posed by surface contacts moving in busy ports and waterways. In order to achieve this goal, the MAS has three main objectives:

1. To help the human operator monitor high volume traffic conditions in the port and surrounding waterways
2. To monitor that vessels comply with the safety and security rules of the port and waterways
3. To help the decision maker identify suspicious behaviors by surface contacts

The thesis is only a preliminary investigation into the modeling of surface contact intent. The intent models are not considered exhaustive as they only use a very small and basic set of parameters and track attributes. It is expected that there will be many more parameters that may be used by human experts in determining the intent of surface contacts.

The focus of this validation will only be on the intent models of the MAS only. The mock VTS-C2 simulator program is only meant to demonstrate the features of the MAS.

Your Background

Country: _____

Rank: _____

Name (optional): _____

E-mail (optional): _____

Number of years of Surface Warfare experience: _____

Number of years of At-Sea/Patrol experience: _____

Objective 1.0

To help the human operator monitor high volume traffic conditions in the port and surrounding waterways

- Based on your experience, how important is this objective?
- Based on your opinion, how did the MAS perform in addressing this objective?
- Please circle your answers for both the importance of the objective and the MAS performance.
- Please also state any comments on how the MAS performance can be improved further with respect to this objective.

Objectives	Importance of objective					MAS performance				
	Not important				Very Important	Poor				Good
1.0 To help the human operator monitor high volume traffic conditions in the port and surrounding waterways	1	2	3	4	5	1	2	3	4	5
Comments:										
1.1 To monitor multiple surface contacts of all types **(PCG, military, cruise liners, leisure, tankers, fishing, oiler)**	1	2	3	4	5	1	2	3	4	5
Comments:										
1.2 To monitor multiple security zones of **HVUs** (High Value Units) **(cruise liners, tankers)**	1	2	3	4	5	1	2	3	4	5
Comments:										
1.3 To monitor **restricted areas (oil refineries, cruise center, military installations)**	1	2	3	4	5	1	2	3	4	5
Comments:										

Objective 2.0

To monitor that vessels comply with the safety and security rules of the port and waterways

- Based on your experience, how important is this objective?
- Based on your opinion, how well did the MAS perform in achieving this objective?
- Please circle your answers for both the importance of the objective and the MAS performance.
- Please also state any comments on how the MAS performance can be improved further with respect to this objective.

Objectives	**Importance of objective**					**MAS performance**				
	Not important				**Very Important**	**Poor**				**Good**
2.0 To monitor that vessels comply with the safety and security rules of the port and waterways	1	2	3	4	5	1	2	3	4	5
Comments:										
2.1 To check for **current** track violations	1	2	3	4	5	1	2	3	4	5
Comments:										
2.1.1 **Current** incursions into the security zones of **HVUs (cruise liners, tankers)**	1	2	3	4	5	1	2	3	4	5
Comments:										
2.1.2 To check for **current** incursions into **restricted areas (cruise center, oil refineries, military installations)**	1	2	3	4	5	1	2	3	4	5
Comments:										

Objectives	Importance of objective					MAS performance				
	Not important				Very Important	Poor				Good
2.1.3 To check for illegal activities in restricted areas	1	2	3	4	5	1	2	3	4	5
Comments:										
2.1.3.1 Fishing in a non-fishing zone	1	2	3	4	5	1	2	3	4	5
Comments:										
2.1.3.2 Cruising in an Area To Be Avoided (ATBA)	1	2	3	4	5	1	2	3	4	5
Comments:										
2.1.4 To check for Traffic Separation Scheme (TSS) violations	1	2	3	4	5	1	2	3	4	5
Comments:										
2.1.4.1 Traveling against traffic direction	1	2	3	4	5	1	2	3	4	5
Comments:										
2.1.4.2 Stopping in a traffic lane	1	2	3	4	5	1	2	3	4	5
Comments:										
2.1.4.3 Stopping in a TSS termination zone	1	2	3	4	5	1	2	3	4	5
Comments:										
2.1.5 To check for speed violations in restricted areas	1	2	3	4	5	1	2	3	4	5
Comments:										

Objectives	Importance of objective					MAS performance				
	Not important				Very Important	Poor				Good
2.1.5.1 Speed violation in a harbor	1	2	3	4	5	1	2	3	4	5
Comments:										
2.1.5.2 Speed violations in a traffic lane	1	2	3	4	5	1	2	3	4	5
Comments:										
2.1.6 To check for Vessel Traffic Service (VTS) violations	1	2	3	4	5	1	2	3	4	5
Comments:										
2.1.6.1 Collision detection	1	2	3	4	5	1	2	3	4	5
Comments:										
2.2 To check for **future** track violations	1	2	3	4	5	1	2	3	4	5
Comments:										
2.2.1 To check for **future** incursions into the security zones of **HVUs (cruise liners, tankers)** using Closest Point of Approach (CPA) and Time to CPA	1	2	3	4	5	1	2	3	4	5
Comments:										
2.2.2 To check for **future** incursions into **restricted areas (cruise center, oil refineries, military installations)**	1	2	3	4	5	1	2	3	4	5
Comments:										

Objective 3.0

To help the decision maker identify suspicious or potentially hostile surface contacts

- Based on your experience, how important is this objective?
- Based on your opinion, how did the MAS perform in addressing this objective?
- Please circle your answers for both the importance of the objective and the MAS performance.
- Please also state any comments on how the MAS performance can be improved further with respect to this objective.

Objectives	Importance of objective					MAS performance				
	Not important				Very Important	Poor				Good
3.0 To help the decision maker identify suspicious or potentially hostile surface contacts	1	2	3	4	5	1	2	3	4	5
Comments:										
3.1 To find atypical track behaviors	1	2	3	4	5	1	2	3	4	5
Comments:										
3.1.1 To check for excessive speed based on track types **(fishing, leisure)**	1	2	3	4	5	1	2	3	4	5
Comments:										
3.1.2 To check for excessive number of track violations	1	2	3	4	5	1	2	3	4	5
Comments:										
3.1.3 To detect participation in coordinated attacks	1	2	3	4	5	1	2	3	4	5
Comments:										

Objectives	Importance of objective					MAS performance				
	Not important				Very Important	Poor				Good
3.1.3.1 To detect coordinated attack (swarm/"wolf-pack") on a HVU/restricted area	1	2	3	4	5	1	2	3	4	5
Comments:										
3.2 To determine threat level posed by surface contact	1	2	3	4	5	1	2	3	4	5
Comments:										
3.2.1 To perform surface threat assessment based on track's attributes	1	2	3	4	5	1	2	3	4	5
Comments:										
3.2.1.1 Threat assessment based on **Track Type**	1	2	3	4	5	1	2	3	4	5
Comments:										
3.2.1.2 Threat assessment based on **Track Flag**	1	2	3	4	5	1	2	3	4	5
Comments:										
3.2.1.3 Threat assessment based on **Track Origin**	1	2	3	4	5	1	2	3	4	5
Comments:										
3.2.1.4 Threat assessment based on **Track Destination**	1	2	3	4	5	1	2	3	4	5
Comments:										

Objectives	Importance of objective					MAS performance				
	Not important				Very Important	Poor				Good
3.2.1.5 Threat assessment based on **Track ESM (Unknown, No emitter, I-Band, X-Band, Others)**	1	2	3	4	5	1	2	3	4	5
Comments:										
3.2.1.6 Threat assessment based on **Voice Communication with Track(Yes, No)**	1	2	3	4	5	1	2	3	4	5
Comments:										
3.3 To adapt to the needs of the decision maker	1	2	3	4	5	1	2	3	4	5
Comments:										
3.3.1 To provide user-defined biases (weights)	1	2	3	4	5	1	2	3	4	5
Comments:										
3.3.2 To incorporate regional intelligence (5 x MARSEC levels) biases	1	2	3	4	5	1	2	3	4	5
Comments:										

Future Enhancements

These are possible future enhancements that may be added to the MAS

- Based on your opinion/experience, how important are these enhancements?
- Please also state any comments on how the enhancements can be implemented.

Future Enhancements	Importance of enhancement				
	Not important				Very Important
1. Detect more track maneuvers	1	2	3	4	5
Comments:					
1.1 Detect unusual zig-zags track maneuvers	1	2	3	4	5
Comments:					
1.2 Detect course changes (of a suspected track to match movements of a HVU	1	2	3	4	5
Comments:					
1.3 Monitor course/heading of tracks in further detail (e.g. in terms of Steady and closing/opening or Turn to closing/opening)	1	2	3	4	5
Comments:					
1.4 Detect hiding/evading from Police Coast Guards (PCG)/military patrols	1	2	3	4	5
Comments:					
2. Check for additional VTS violations	1	2	3	4	5
Comments:					
2.1 Failure to submit Offshore Advance reports	1	2	3	4	5
Comments:					

Future Enhancements	Importance of enhancement				
	Not important				Very Important
2.2 Unknown/wrong destination	1	2	3	4	5
Comments:					
3. Detect more coordinated activities	1	2	3	4	5
Comments:					
3.1 Detect simultaneous attacks on multiple HVUs or restricted areas	1	2	3	4	5
Comments:					
4. Incorporate more specific regional intelligence	1	2	3	4	5
Comments:					
4.1 Specific intelligence based on track attributes **(track type, origin, activity)**	1	2	3	4	5
Comments:					
4.2 Specific intelligence based on historical data (e.g. piracy reports)	1	2	3	4	5
Comments:					
5. Proactive search by agents for more track information i.e. form a paper trail from information sources such as databases of ship registration, sail plans, Offshore Advance reports, cargo/passenger manifests etc	1	2	3	4	5
Comments:					

Do you have any additional comments/suggested enhancements for the MAS:

End of Questionaire

Thank you very much for your participation

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Tan, Chee Ping
   Defence Science and Technology Agency
   Defence Technology Tower A
   Singapore

4. Chew, Lock Pin
   Defence Science and Technology Agency
   Defence Technology Tower A
   Singapore

5. John Hiles
   Naval Postgraduate School
   Monterey, California

6. Russell Gottfried
   Lockheed Martin Space Systems
   Sunnyvale, California

7. CAPT Jeffrey E. Kline, USN
   Naval Postgraduate School
   Monterey, California

8. Dr Thomas V. Huynh
   Naval Postgraduate School
   Monterey, California

9. LTC Eugene P. Paulo, USA
   Naval Postgraduate School
   Monterey, California

10. CAPT Stephen Starr King, USN
    Naval Postgraduate School
    Monterey, California

11. R. Mitchell Brown, III
U.S. Naval War College
Monterey, California

12. Mike McMaster
Naval Postgraduate School
Monterey, California